

KASPERSKY LABS

Kaspersky® Administration Kit 6.0

Guide de déploiement

KASPERSKY® ADMINISTRATION KIT 6.0

Guide de déploiement

© Kaspersky Lab Ltd.
Tél./fax : +7 (495) 797-87-00
<http://www.kaspersky.com/fr>

Date d'édition: Février 2007

Table des matières

CHAPITRE 1. KASPERSKY® ADMINISTRATION KIT	5
1.1. Présentation de Kaspersky Administration Kit	5
1.2. Configuration requise	7
1.3. Contenu du pack logiciel	9
1.4. Services réservés aux utilisateurs enregistrés	9
1.5. Objectif du document	9
1.6. Conventions utilisées dans cet ouvrage	10
CHAPITRE 2. STRATEGIES TYPQUES DE DEPLOIEMENT DE LA PROTECTION ANTIVIRUS	11
2.1. Modes de diffusion de la protection antivirus sur les postes du réseau logique	11
2.2. Construction d'un système d'administration centralisé de la protection antivirus.	12
CHAPITRE 3. INSTALLATION DE KASPERSKY® ADMINISTRATION KIT	14
3.1. Installation de MSDE au départ du fichier d'installation de Kaspersky Administration Kit	16
3.2. Installation du serveur d'administration et de la console d'administration en local sur le poste	18
3.3. Désinstallation des composants de Kaspersky Administration Kit	35
3.4. Mise à jour vers une version plus récente de l'application	35
CHAPITRE 4. INSTALLATION ET DESINSTALLATION D'APPLICATIONS SUR DES POSTES CLIENTS	37
4.1. Installation à distance du logiciel	38
4.1.1. Création d'un paquet d'installation	40
4.1.2. Affichage configuration des paramètres du paquet d'installation	43
4.1.3. Création et configuration d'un paquet d'installation pour l'agent réseau	46
4.1.4. Création et configuration d'un paquet d'installation pour le serveur d'administration.	50
4.1.5. Création d'une tâche de diffusion du paquet d'installation sur les serveurs d'administration secondaires	50

4.1.6. Diffusion des paquets d'installation dans les limites du groupe à l'aide d'agents d'administration	52
4.1.7. Création d'une tâche d'installation à distance	55
4.1.8. Configuration de la tâche d'installation à distance.....	67
4.1.9. Installation à distance d'une application sur les serveurs d'administration secondaires	69
4.1.10. Désinstallation à distance d'une application	72
4.2. Assistant de déploiement d'application.....	73
4.3. Installation locale des applications.....	77
4.3.1. Installation locale de l'agent réseau	78
4.3.2. Installation locale du plug-in d'administration des applications	83
4.3.3. Installation d'applications en mode silencieux	84
ANNEXE A. GLOSSAIRE	86
ANNEXE B. KASPERSKY LAB	93
B.1. Autres produits antivirus	94
B.2. Coordonnées.....	105
ANNEXE C. CONTRAT DE LICENCE	107

CHAPITRE 1. KASPERSKY®

ADMINISTRATION KIT

1.1. Présentation de Kaspersky Administration Kit

Kaspersky Administration Kit est une application développée pour exécuter, de manière centralisée, les principales tâches d'administration de la sécurité des ordinateurs du réseau d'une entreprise. Il repose sur les applications faisant partie de la suite Kaspersky Business Optimal et Kaspersky Corporate Suite. Kaspersky Administration Kit est compatible avec toutes les configurations de réseaux qui utilisent le protocole TCP/IP.

Kaspersky Administration Kit est un outil pour administrateurs de réseaux d'entreprise et pour responsables de sécurité antivirus.

Il propose aux administrateurs les fonctions suivantes :

- Installation et désinstallation centralisée à distance d'applications de Kaspersky Lab sur les postes du réseau. L'administrateur peut copier une fois sur un ordinateur sélectionné l'ensemble d'applications de Kaspersky Lab avant de procéder à l'installation à distance sur les ordinateurs du réseau.
- Administration centralisée à distance des applications de Kaspersky Lab. Cela permet de créer une protection antivirus à plusieurs niveaux et d'administrer toutes les applications depuis le poste de travail de l'administrateur. Ceci est particulièrement intéressant pour les grandes entreprises dont l'intranet peut contenir un nombre élevé de postes répartis en divers bâtiments. Cette fonction couvre :
 - La consolidation des postes au sein de *groupes d'administration* selon les fonctions exécutées et les applications installées.
 - La configuration centralisée des paramètres de fonctionnement de l'application à l'aide de la création et de l'application de *stratégies de groupes*.
 - La configuration individuelle des paramètres de fonctionnement de l'application pour des ordinateurs distincts à l'aide des *paramètres de l'application* ;

- L'administration centralisée de l'application à l'aide de la création et du chargement de *tâches de groupes et de tâches globales*.
- La constitution de modes de fonctionnement individuels pour les applications à l'aide de la création et du lancement de tâches pour une sélection d'ordinateurs issus de divers groupes d'administration.
- Mise à jour automatique des bases antivirus et des modules de l'application sur les ordinateurs. Il est possible de procéder à la mise à jour centralisée des bases antivirus pour toutes les applications installées sans que chaque poste du réseau ne doive contacter le serveur de Kaspersky Lab. La mise à jour peut se dérouler automatiquement selon l'horaire défini par l'administrateur. Ce dernier peut également surveiller la diffusion des mises à jour sur les postes clients.
- Constitution de rapports. Cette fonction permet de recueillir les statistiques relatives au fonctionnement de toutes les applications installées, de veiller à leur bon état et de générer des rapports sur la base des informations obtenues. L'administrateur peut créer un rapport de réseau unique pour l'application ou des rapports sur le fonctionnement de l'application sur chaque poste.
- Mécanisme de notification d'événements. Mécanisme de diffusion des événements. L'administrateur peut constituer une liste d'événements entraîneront l'envoi d'une notification. Par exemple, la découverte d'un virus, l'échec de la mise à jour des bases antivirus ou la découverte d'un nouveau poste dans le réseau.
- Gestion des clés de licences. Cette fonction permet d'installer de manière centralisée les clés de licence pour toutes les applications installées, de veiller au respect du contrat de licence (nombre de licences correspondant au nombre d'applications installées sur le réseau) et de contrôler les dates d'expiration.
- Collaborer avec le système Cisco Network Admission Control (NAC). Cette fonction permet d'introduire les correspondances entre les conditions de protection antivirus de l'ordinateur et les états Cisco NAC.

Kaspersky Administration Kit renferme les trois composants suivants :

- **Serveur d'administration** qui joue le rôle de centre d'informations centralisé sur les applications de Kaspersky Lab installées sur les postes du réseau de l'entreprise et permettant de les administrer.
- **Agent réseau** assure l'interaction entre le serveur d'administration et les applications de Kaspersky Lab installées sur un nœud particulier du

réseau (poste de travail ou serveur). Ce composant est unique pour toutes les applications Windows des suites Kaspersky Anti-Virus Business Optimal et Kaspersky Corporate Suite. Il existe des versions de l'agent réseau spécifiques aux applications Kaspersky Lab tournant sur Novell ou Unix.

- La **Console d'administration** fournit l'interface utilisateur nécessaire pour les services d'administration du serveur et de l'agent. Le module de gestion se présente sous la forme d'une extension à la Microsoft Management Console (MMC).

1.2. Configuration requise

Serveur d'administration

- Configuration logicielle :
 - Microsoft Data Access Components (MDAC) version 2.8 et suivante;
 - MSDE 2000 avec Service Pack 3 ou suivant, Microsoft SQL Server 2000 avec Service Pack 3¹ ou suivant, MySQL version 5.0.22 (code de page par défaut, UTF-8), Microsoft SQL 2005 et suivant ou Microsoft SQL 2005 Express ou suivant ;
 - Microsoft Windows 2000 avec Service Pack 1 ou suivant; Microsoft Windows XP Professional avec Service Pack 1 ou suivant; Microsoft Windows XP Professional x64 ou suivant; Microsoft Windows Server 2003 ou suivant; Microsoft Windows Server 2003 x64 ou suivant; Microsoft Windows NT4 avec Service Pack 6a ou suivant, Microsoft Windows Vista.
- Configuration matérielle :
 - Processeur Intel Pentium III de 800 Mhz minimum ;
 - 128 Mo de RAM ;
 - 400 Mo d'espace disponible sur le disque.

Console d'administration

- Configuration logicielle :

¹ L'installation de MSDE peut s'effectuer à l'aide de la distribution livrée avec Kaspersky Administration Kit.

- Microsoft Windows 2000 avec Service Pack 1 ou suivant; Microsoft Windows XP Professional avec Service Pack 1 ou suivant; Microsoft Windows XP Home Edition avec Service Pack 1 ou suivant; Microsoft Windows XP Professional x64 ou suivant; Microsoft Windows Server 2003 ou suivant; Microsoft Windows Server 2003 x64 ou suivant; Windows NT4 avec Service Pack 6a ou suivant, Microsoft Windows Vista ;
- Microsoft Management Console version 1.2 ou suivante.
- Configuration matérielle :
 - Processeur Intel Pentium II de 400 Mhz minimum ;
 - 64 Mo de RAM ;
 - 10 Mo d'espace disponible sur le disque.

Agent réseau

- Configuration logicielle :
- Pour les systèmes Windows :

Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 avec Service Pack 1 ou suivant; Microsoft Windows NT4 avec Service Pack 6a ou suivant; Microsoft Windows XP Professional avec Service Pack 1 ou suivant; Microsoft Windows XP Professional x64 ou suivant; Microsoft Windows Server 2003 ou suivant; Microsoft Windows Server 2003 x64 ou suivant.
- Pour les systèmes Novell :

Novell NetWare 6 SP3 ou suivant ; Novell NetWare 6.5 SP3 ou suivant.
- Configuration matérielle :
- Pour les systèmes Windows :
 - processeur Intel Pentium I de 233 Mhz minimum ;
 - 32 Mo de RAM ;
 - 10 Mo d'espace disponible sur le disque.
- Pour les systèmes Novell :
 - processeur Intel Pentium I de 233 Mhz minimum ;
 - 12 Mo de RAM ;
 - 32 Mo d'espace disponible sur le disque.

1.3. Contenu du pack logiciel

Ce progiciel est accompagné gratuitement toutes les applications de Kaspersky Lab distribuées avec Kaspersky Anti-Virus Business Optimal et Kaspersky Corporate Suite (version vendue en boîte) et se trouve également disponible pour la vente sur le site de Kaspersky Lab à l'adresse www.kaspersky.ru.

1.4. Services réservés aux utilisateurs enregistrés

Kaspersky Lab propose un large éventail de services à ses utilisateurs inscrits leur permettant d'utiliser plus efficacement les produits Kaspersky Lab .

Quand vous achetez la licence de l'un des produits Kaspersky Lab inclus dans Kaspersky Anti-Virus Business Optimal ou dans Kaspersky Corporate Suite, vous devenez un utilisateur inscrit de Kaspersky Administration Kit. Par la suite vous pourrez bénéficier des services suivants pour la durée de votre licence :

- Nouvelles versions de ce logiciel antivirus, fournies gratuitement ;
- Assistance téléphonique et par formulaire pré-rempli sur le Web sur l'installation, la configuration et l'utilisation de l'application antivirus ;

Avant de soumettre une consultation au service d'assistance technique, assurez-vous de connaître les informations de licence relatives aux applications de Kaspersky Lab utilisée avec Kaspersky Administration Kit.

- Informations sur les nouveaux produits Kaspersky Lab et les nouveaux virus d'ordinateurs (pour les abonnés au bulletin).

Kaspersky Lab ne fournit pas d'informations concernant l'administration ou l'utilisation de votre système d'exploitation ou d'autres technologies.

1.5. Objectif du document

Ce livre de référence présente l'usage de Kaspersky Administration Kit et contient des explications pas à pas de toutes ses fonctions. Les principes de base et le schéma de fonctionnement généraux de l'application sont décrits dans le Guide de l'administrateur de Kaspersky Administration Kit.

Pour lire les questions les plus fréquentes que nos utilisateurs posent aux spécialistes du service support de Kaspersky Lab, visitez notre site Web et suivez le lien **Services→ Banque de solutions**. Cette section contient des informations sur l'installation, la configuration et le fonctionnement des

applications Kaspersky Lab, sur la suppression des virus les plus répandus, ainsi que sur la désinfection des fichiers infectés.

1.6. Conventions utilisées dans cet ouvrage

Plusieurs conventions ont été adoptées dans ce guide en fonction du contenu et de l'intérêt de chaque section particulière. Le tableau ci-après illustre les conventions utilisées dans ce manuel.

Mise en forme	Signification / Usage
Gras	Titres de menus et de fenêtres, commandes, éléments de boîte de dialogue, etc.
<i>Note.</i>	Information complémentaire, remarques
Attention !	Informations nécessitant une attention particulière
<i>Pour exécuter...,</i> 1. Étape 1. 2. ...	Description de la succession des étapes que l'utilisateur doit suivre et des actions possibles.
Tâche ou exemple	Définition d'un problème, exemple ou démonstration des possibilités de l'application
[option] – nom du paramètre	Paramètre de ligne de commande.
Texte des messages d'information et de la ligne de commande	Texte des fichiers de configuration, des messages d'information et de la ligne de commande.

CHAPITRE 2. STRATÉGIES TYPIQUES DE DEPLOIEMENT DE LA PROTECTION ANTIVIRUS

2.1. Modes de diffusion de la protection antivirus sur les postes du réseau logique

Il existe deux modes de déploiement des systèmes de protection antivirus gérés via Kaspersky Administration Kit :

- Via l'installation à distance centralisée de l'application sur les postes client du réseau logique. Dans ce cas, l'installation de l'application et la connexion au système d'administration centralisée à distance se produisent automatiquement sans aucune intervention de l'administrateur et il est possible d'installer un logiciel antivirus sur n'importe quel nombre de postes client.
- Via l'installation locale de l'application sur chaque poste client. Dans ce cas, l'installation des composants indispensables sur les postes client et sur le poste de travail de l'administrateur s'opère manuellement et les paramètres de connexion des postes clients au serveur d'administration sont définis lors de l'installation de l'agent réseau. Cette option est à conseiller uniquement lorsque l'installation centralisée à distance est impossible.

L'installation à distance peut servir à l'installation de n'importe quelle application choisie par l'utilisateur. Toutefois, Kaspersky Administration Kit prend uniquement en charge l'administration des applications de Kaspersky Lab dotée du composant spécial qu'est le module externe d'administration.

2.2. Construction d'un système d'administration centralisé de la protection antivirus.

La première étape lors de la constitution d'un système d'administration centralisé de la protection antivirus du réseau de l'entreprise à l'aide de Kaspersky Administration Kit consiste à prévoir le réseau logique. Cette étape suppose la prise des décisions suivantes :

1. Identifier des parties isolées du réseau et décider du nombre de serveurs d'administration qui seront nécessaires. Le recours à la hiérarchie du serveur d'administration permet de réduire considérablement la charge des canaux de communication et d'augmenter la fiabilité du système.
2. Quels seront les postes du réseau de l'entreprise qui rempliront les fonctions de serveur d'administration principal et de serveurs d'administration secondaires, quels postes de travail de l'administrateur et quels postes clients. Les postes clients sont tous les ordinateurs sur lesquels il est prévu d'installer les applications de Kaspersky Lab.
3. Quel signe entraînera l'actualisation des postes clients du groupe et quelle sera la hiérarchie du groupe.
4. Quel sera le mode de déploiement du système de protection antivirus choisi : installation locale ou à distance.

Au cours de l'étape suivante, l'administrateur doit créer le réseau logique en installant les composants correspondant de Kaspersky Administration Kit sur les postes du réseau, à savoir :

1. Installer les serveurs d'administration sur les ordinateurs repris dans le réseau de l'entreprise.
2. Installer la console d'administration sur les ordinateurs au départ desquels l'administration sera réalisée.
3. Désigner les administrateurs du réseau logique, définir les catégories d'utilisateurs qui utiliseront le système et définir pour chaque catégorie la liste des fonctions qui pourront être remplies.

4. Constituer des groupes d'utilisateurs et octroyer à chacun d'entre eux les privilèges nécessaires à l'exécution des tâches des utilisateurs qui en font partie.

Ensuite, il conviendra de créer la hiérarchie du serveur d'administration et de composer pour chacun de ces serveurs la structure du réseau logique : construire la hiérarchie des groupes d'administration et répartir les postes dans les groupes correspondant.

L'étape suivante consiste à installer l'agent réseau sur les postes client ainsi que les applications indispensables de Kaspersky Lab et les modules externes d'administration des applications correspondantes sur le poste de travail de l'administrateur.

Lors de l'utilisation de l'installation à distance, l'agent réseau peut être installé avec n'importe quelle application. Dans ce cas, il n'est pas nécessaire de procéder à une installation séparée de l'agent réseau.

La dernière étape correspond à la configuration des applications installées à l'aide de la définition et de l'application de stratégies de groupe et de la création des tâches indispensables.

L'application offre la possibilité de créer un système d'administration centralisée de la protection antivirus avec un minimum de configuration grâce à l'assistant de configuration initiale. Il est également possible de créer un réseau logique identique à la structure du domaine du réseau Windows et de créer un système de protection antivirus à l'aide de Kaspersky Anti-Virus for Windows Workstations version 5.0 et 6.0.

CHAPITRE 3. INSTALLATION DE KASPERSKY® ADMINISTRATION KIT

Avant de vous lancer dans la procédure d'installation, assurez-vous que votre ordinateur répond aux critères de configuration matérielle et logicielle définis pour le serveur d'administration et le poste de travail de l'administrateur (cf. point 1.3, p. 9).

Le serveur d'administration conserve les données dans MSDE (Microsoft Data Engine), un serveur MySQL ou un serveur Microsoft SQL. Si MSDE ou un serveur SQL n'est pas installé dans le réseau de l'entreprise, il faudra d'abord l'installer avant de poursuivre l'installation du serveur d'administration. Vous pouvez pour ce faire utiliser les fichiers d'installation dont vous disposez. S'agissant de l'installation de MSDE, vous pouvez également utiliser le fichier d'installation de Kaspersky Administration Kit. Vous trouverez ci-après (cf. point 3.1, p. 16) la description de la procédure d'installation de MSDE au départ du fichier d'installation de Kaspersky Administration Kit.

Vous devez jouir des privilèges d'administrateur sur le poste où vous comptez installer Kaspersky Administration Kit.

Le programme d'installation vous propose d'installer sur l'ordinateur utilisé les composants logiciels de Kaspersky Administration Kit, à savoir le serveur d'administration et la console d'administration. Cette configuration est recommandée au début de la constitution d'un système de gestion centralisée à distance.

Pour garantir le bon fonctionnement des composants applicatifs après l'installation, il est indispensable d'ouvrir une série de ports sur les ordinateurs. Le tableau 1 reprend la liste des ports qu'utilise par défaut Kaspersky Administration Kit.

Tableau 1

Numéro du port	Protocole	Description
Ordinateur sur lequel est installé le serveur d'administration		
13000	TCP et UDP	En combinaison avec le protocole SSL, permet de : <ul style="list-style-type: none"> la réception des données des postes clients ; la connexion des agents de mise à jour ; la connexion des serveurs d'administration secondaires ; la réception des avis de déconnexion des ordinateurs.
13292	TCP	Utilisé pour la connexion de périphériques mobiles. ²
14000	TCP	Est utilisé pour : <ul style="list-style-type: none"> la réception des données des postes clients ; la connexion des agents de mise à jour ; la connexion des serveurs d'administration secondaires.
18000	HTTP	Permet au serveur d'administration de recevoir les données d'authentification du serveur Cisco NAC.
Ordinateur sur lequel est installé l'agent de mises à jour		
13000	TCP	Permet la connexion des postes clients.
13001	TCP	Permet la connexion des postes clients lorsque l'ordinateur est à la fois agent de mises à jour et serveur d'administration.
14000	TCP	Permet la connexion des postes clients.

² Par périphérique mobile, il faut comprendre un appareil équipé de Kaspersky Anti-Virus 6.0 Mobile Enterprise Edition.

14001	TCP	Permet la connexion des postes clients lorsque l'ordinateur est à la fois agent de mises à jour et serveur d'administration.
Poste client sur lequel est installé l'agent réseau		
15000	UDP	Permet de traiter les demandes de connexion au serveur d'administration.

3.1. Installation de MSDE au départ du fichier d'installation de Kaspersky Administration Kit

Avant de procéder à l'installation de MSDE, il convient d'installer Microsoft Data Access Components (MDAC) version 2.8 ou suivante (le fichier d'installation est disponible sur le site de Microsoft).

L'installation de MSDE au départ du fichier d'installation de Kaspersky Administration Kit s'opère localement.

Pour installer MSDE :

1. Lancez le fichier exécutable qui se trouve dans le répertoire **MSDE2KSP3** du cédérom d'installation de Kaspersky Administration Kit. L'Assistant d'installation vous proposera de configurer les paramètres avant de passer à l'exécution. Suivez les instructions affichées.
2. Les premières étapes de l'installation sont standard et consistent à décompacter tous les fichiers indispensables et à les enregistrer sur le disque dur de l'ordinateur, à vérifier l'installation des applications indispensables, à accepter le contrat de licence et à saisir les informations relatives à l'utilisateur ou à l'entreprise.
3. Dans la boîte de dialogue **Sélectionnez l'emplacement cible**, définissez :
 - Le répertoire d'installation des fichiers de MSDE dans le champ **Modules du logiciel**. Il s'agit par défaut de **<Disque>:\Program Files\Microsoft SQL Server**. Si ce répertoire n'existe pas, il sera créé automatiquement.
 - Le répertoire qui accueillera les bases de données du serveur MSDE dans le champ **Base de données**. Il s'agit par défaut

également de <Disque>:\Program Files\Microsoft SQL Server.

Cliquez sur **Parcourir** pour sélectionner les différents répertoires.

4. Ensuite, dans la boîte de dialogue **Nom du serveur SQL** (cf. ill. 1), saisissez le nom qui sera attribué à ce serveur.

Aucun nom n'est proposé par défaut. Le serveur sera désigné par le nom de l'ordinateur sur lequel il est installé.

Si vous souhaitez définir un autre nom, désélectionnez la case **Par défaut** et saisissez le nouveau nom dans le champ **Nom d'instance**. Une fois que les paramètres auront été définis, vous pouvez les vérifier et lancer l'installation. Si tout se passe comme il le faut, MSDE sera installé sur votre ordinateur.

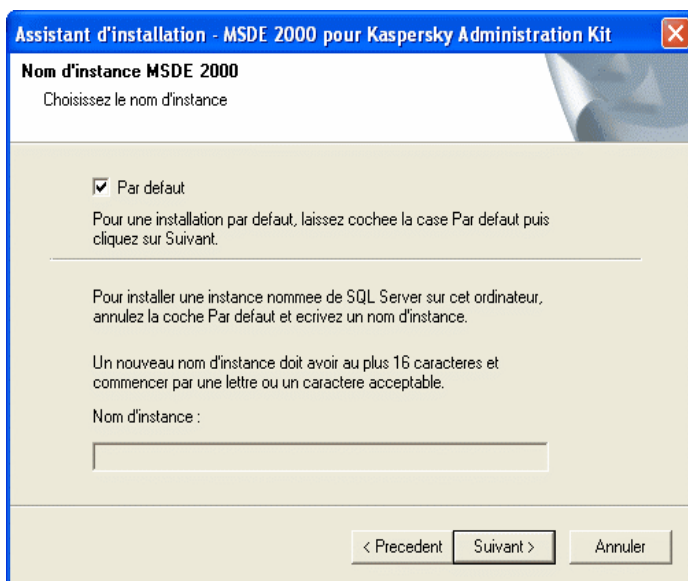


Illustration 1. Sélection du nom du serveur

3.2. Installation du serveur d'administration et de la console d'administration en local sur le poste

Ce chapitre décrit la procédure d'installation locale du serveur et/ou de la console d'administration. Si un serveur d'administration est déjà installé sur le réseau, l'installation d'autres serveurs peut être effectuée à l'aide d'une tâche d'installation à distance, qu'on appelle installation forcée (voir section 4.1.7 à la page 24). Pour créer cette tâche, utilisez le paquet d'installation du serveur d'administration (voir section 4.1.4 à la page 24).

Pour installer le serveur d'administration et/ou la console d'administration en local sur le poste :

1. Lancez le fichier **setup.exe** qui se trouve sur le cédérom d'installation. L'Assistant d'installation vous proposera de configurer différents paramètres. Suivez les instructions affichées.
2. Les premières étapes correspondent au décompactage des fichiers indispensables et à leur enregistrement sur le disque dur, à l'acceptation du contrat de licence et à la saisie d'informations sur l'utilisateur et l'entreprise.
3. Indiquez ensuite le répertoire d'installation des composants. Il s'agit par défaut de **<Disque>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit**. Si ce répertoire n'existe pas, il sera créé automatiquement. Cliquez sur **Parcourir** pour sélectionner un autre répertoire.
4. **Sélectionnez** ensuite les composants de Kaspersky Administration Kit que vous souhaitez installer (cf. ill. 2) :
 - **Serveur d'administration.** Le cas échéant, permet d'installer les composants standard Kaspersky Lab permettant la collaboration avec Cisco NAC. Pour ce faire, cochez la case **Posture Validation Server Kaspersky Lab pour Cisco NAC**. Il est possible de configurer les paramètres de collaboration Cisco NAC dans les propriétés ou la stratégie du serveur d'administration (pour de plus amples détails, voir le Manuel de référence Kaspersky Administration Kit).

- **Console d'administration.**

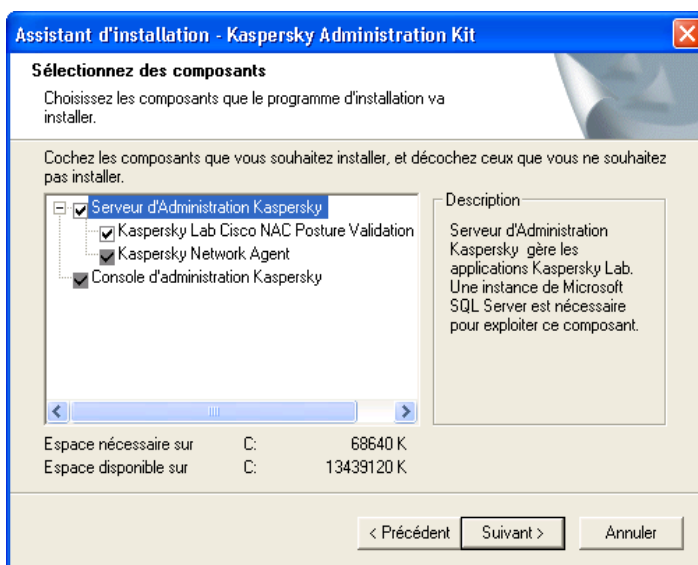


Illustration 2. Sélection des composants à installer

Vous pouvez décider d'installer tous les composants ou uniquement la console d'administration. Il est impossible d'installer le serveur d'administration sans la console d'administration. L'installation de tous les composants est proposée par défaut.

En plus du serveur d'administration, la version serveur de l'agent réseau sera installée sur l'ordinateur. Son installation avec la version standard de l'agent réseau est impossible. Si ce composant est déjà installé sur votre ordinateur, il conviendra de le supprimer avant d'installer le serveur d'administration.

Vous remarquerez que les boîtes de dialogue de l'assistant fournissent des informations d'aide :

- Dans le champ **Description** du composant sélectionné dans la partie droite.
- L'espace disque indispensable à l'installation des composants sélectionnés dans la partie inférieure ainsi que l'espace disponible sur le disque sélectionné.

Si vous avez décidé d'installer uniquement la console d'administration, l'Assistant de configuration s'arrête ici et vous passez directement à la fenêtre de configuration des paramètres et de lancement de l'installation.

5. Si vous avez décidé d'installer le serveur d'administration, définissez à l'étape suivante le compte sous lequel le serveur d'administration sera lancé en tant que serveur sur cet ordinateur (cf. ill. 3).

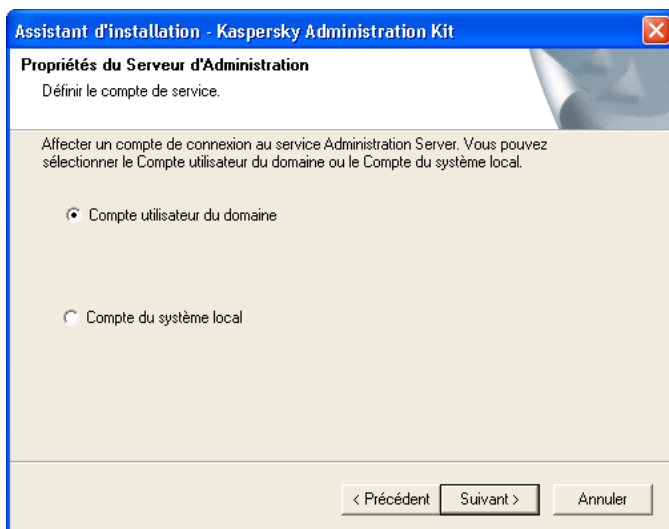


Illustration 3. Sélection du compte

Choisissez l'une des deux options suivantes :

- **Compte utilisateur du domaine** : le serveur d'administration sera exécuté sous le compte utilisateur du domaine. Dans ce cas, le serveur d'administration lancera toutes les opérations avec les privilèges de ce compte et à l'étape suivante, il faudra désigner l'utilisateur dont le compte sera utilisé.

Si une structure de domaines Windows existe dans le réseau, il est conseillé de choisir le compte d'administrateur du domaine pour lancer le serveur d'administration. Vous éviterez ainsi les configurations complémentaires telles que la définition d'un compte utilisateur jouissant de privilèges d'administrateur lors de la création d'une tâche d'installation à distance (cf. point 4.1.7, p. 55).

- **Compte utilisateur système** : le serveur d'administration sera lancé sous le compte **Système local** avec ses privilèges. Dans ce cas, il n'est pas nécessaire de choisir un utilisateur et vous passerez immédiatement à la définition de la ressource de stockage de la base d'informations du serveur d'administration (cf. point n° 7, p. 22)

Pour assurer le bon fonctionnement de Kaspersky Administration Kit, il faut que le compte utilisateur utilisé pour le lancement du serveur d'administration jouisse des privilèges d'administrateur de la ressource de stockage des bases d'informations du serveur d'administration.

6. Si vous avez choisi le compte d'un utilisateur du domaine en guise de compte utilisateur pour le lancement du serveur d'administration, vous devrez définir cet utilisateur.

Pour faire, saisissez le nom d'un utilisateur enregistré dans ce domaine manuellement ou à l'aide du bouton **Parcourir** dans le champ **Nom utilisateur** (cf. ill. 4). Saisissez ensuite le mot de passe utilisé par l'utilisateur pour s'enregistrer dans le domaine.

Assistant d'installation - Kaspersky Administration Kit

Propriétés du Serveur d'Administration
Compte de service

Sélectionnez le compte utilisateur pour le service Administration Server.

Nom d'utilisateur : Parcourir...

Mot de passe :

< Précédent Suivant > Annuler

Illustration 4. Sélection de l'utilisateur

Si vous avez choisi un utilisateur qui ne jouit pas des privilèges d'administrateur du domaine, le serveur d'administration sera lancé sous

son compte mais les fonctions de Kaspersky Administration Kit seront quelque peu réduites. Par exemple, il ne jouit peut-être pas du privilège d'exécution d'une installation à distance à l'aide d'un script de lancement (cf. point 4.1.7, p. 55) ou de sondage de plusieurs domaines du réseau Windows.

Pour garantir le bon fonctionnement du serveur d'administration, le compte utilisé pour son lancement doit également jouir des privilèges suivants :

- Ouverture de session en tant que service (Log on as a service);
- Travail en mode de système d'exploitation (Act as part of the operating system) ;
- Accès à l'ordinateur depuis le réseau (Access this computer from the network);
- Remplacement d'un marqueur de niveau de processus (Replace a process level token) ;
- Configuration de la part de mémoire pour le processus (increase quotas/adjust memory quotas for a process).

Si l'utilisateur que vous avez choisi est un administrateur de domaine qui ne jouit pas des privilèges cités ci-dessus, il les obtiendra (cf. ill. 5)



Illustration 5. Message sur l'octroi de privilèges

7. L'étape suivante consiste à définir la ressource **Microsoft SQL Serveur (MSDE)** ou **MySQL** (cf. ill. 6) qui accueillera la base de données du serveur d'administration.

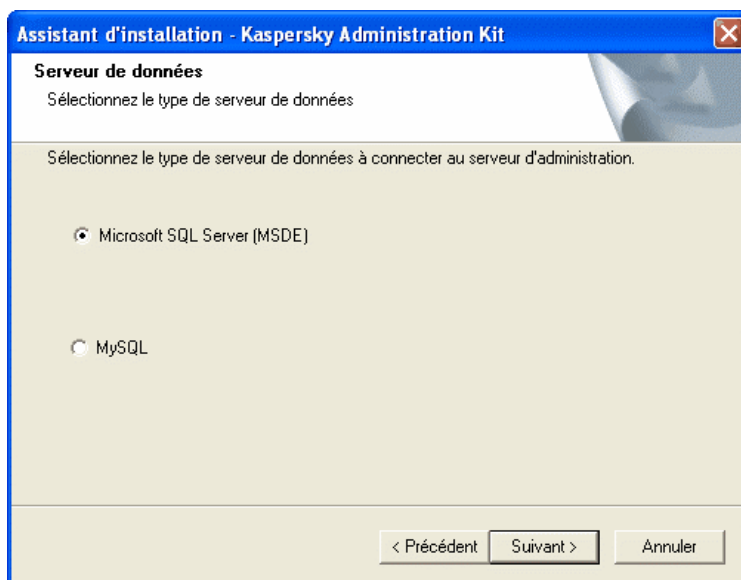


Illustration 6. Sélection des bases de données

8. Si vous avez sélectionné MSDE ou Microsoft SQL Server à l'étape précédente et que vous avez l'intention d'utiliser un serveur installé dans le réseau de l'entreprise pour Kaspersky Administration Kit, indiquez son nom dans le champ **Nom du serveur** et indiquez le nom de la base de données qui sera créée pour stockées les données du serveur d'administration dans le champ **Nom de la base de données** (cf. ill. 7). Le nom de la base de données proposé par défaut est **KAV**.

Le champ **Nom du serveur SQL** prend automatiquement la valeur (**local**) si le serveur est découvert sur l'ordinateur au départ duquel l'installation de Kaspersky Administration Kit est réalisée. A l'aide du bouton **Parcourir**, affichez la liste de tous les serveurs Microsoft SQL installés sur le réseau.

Si le lancement du serveur d'administration va se réaliser sous le compte administrateur local ou sous le compte système, le bouton **Parcourir** n'est pas accessible.

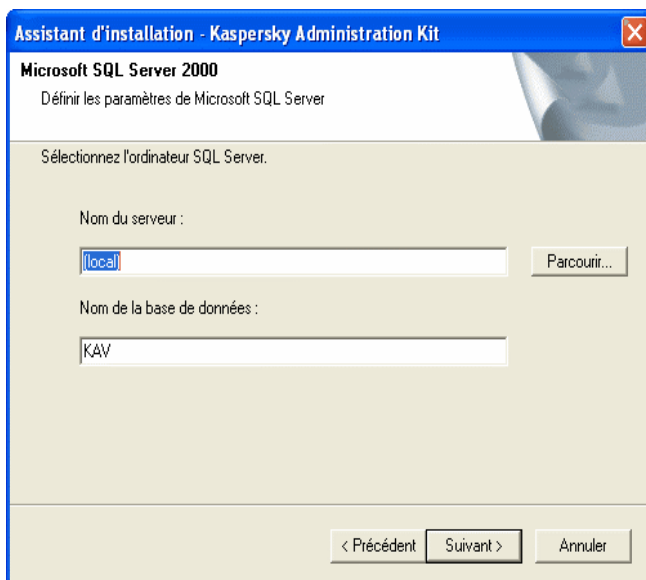


Illustration 7. Sélection du serveur SQL

Si un serveur MySQL a été sélectionné à l'étape précédente, vous devrez indiquer dans cette fenêtre (cf. ill. 8) son nom dans le champ **Nom du serveur** (par défaut, c'est l'adresse IP de l'ordinateur sur lequel est installé Kaspersky Administration Kit qui est utilisée) et définissez le port de connexion dans le champ **Port** (par défaut, il s'agit du port 3306). Dans le champ **Nom de la base de données**, saisissez le nom de la base de données qui sera créée pour stocker les données du serveur d'administrateur (par défaut, le nom de la base de données est **KAV**).

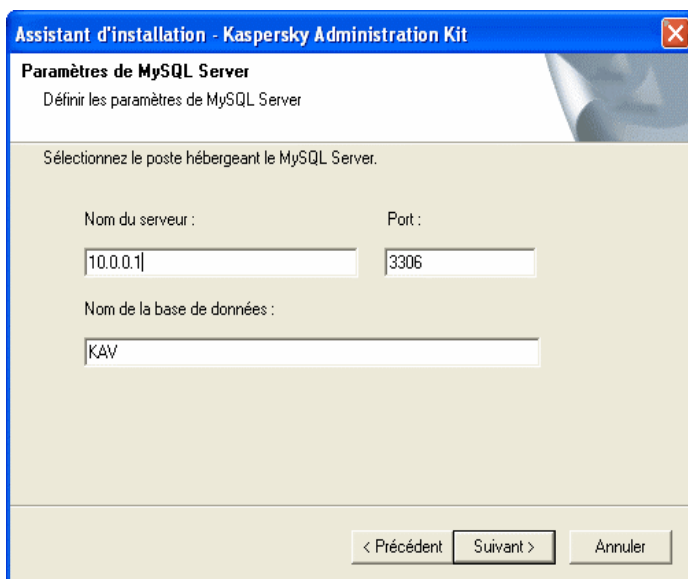


Illustration 8. Sélection du serveur MySQL

Si votre réseau ne possède aucun serveur MS SQL ou que vous ne pouvez pas utiliser de serveur(s) existants, vous devrez alors en installer un (voir section 3.1 à la page 16).

Si vous voulez installer Microsoft SQL Server sur le même ordinateur où vous installez Kaspersky Administration Kit, alors annulez l'installation courante, installez le serveur SQL, puis recommencez l'installation.

Si vous voulez installer Microsoft SQL Server sur un ordinateur à distance, il n'est pas nécessaire d'annuler l'installation de Kaspersky Administration Kit. Vous pouvez installer Microsoft SQL Server et poursuivre l'installation de Kaspersky Administration Kit.

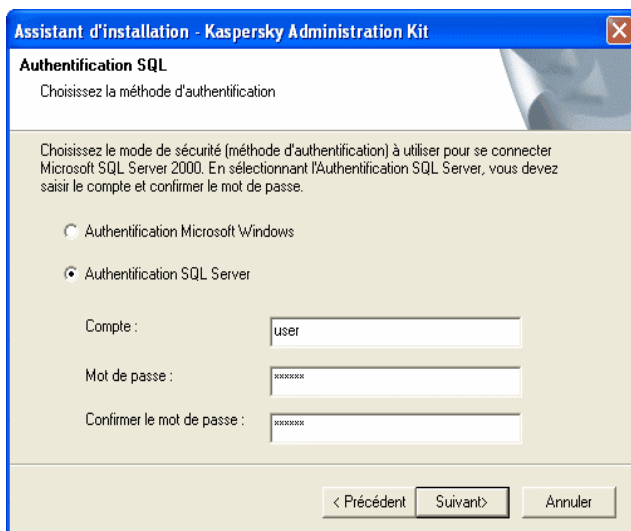
9. Au cours de cette étape vous devez déterminer la méthode d'authentification utilisée pour la connexion du serveur d'administration au serveur SQL.

Pour MSDE ou Microsoft SQL server, vous avez le choix entre les options suivantes (cf. ill. 9):

- **Mode d'authentification Microsoft Windows-** dans ce cas, votre compte est utilisé pour vérifier vos droits d'utilisation du Serveur d'administration;

- **Mode d'authentification SQL Server**- dans ce cas, c'est le compte spécifié à la suite qui sera utilisé pour vérifier les droits. Saisissez le mot de passe dans les champs **Compte**, **Mot de passe** et **Confirmation du mot de passe**.

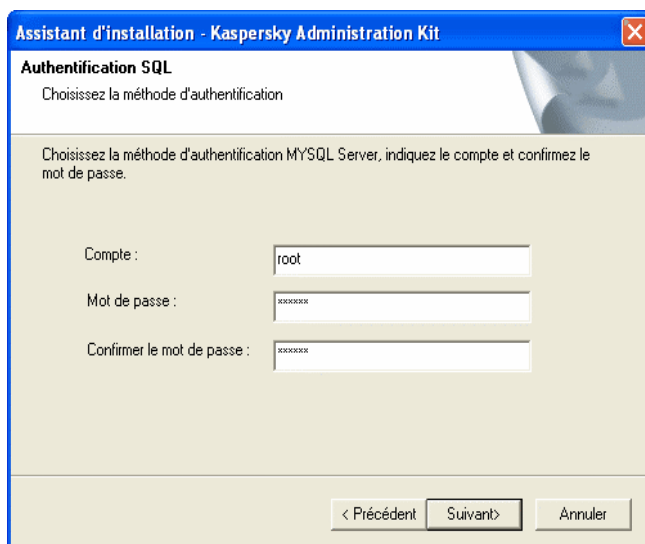
Pour un transfert correct des données sur un nouveau serveur SQL, celui-ci doit avoir les mêmes fusions que le serveur SQL précédent.



The screenshot shows a window titled "Assistant d'installation - Kaspersky Administration Kit" with a close button in the top right corner. The main heading is "Authentification SQL". Below it, the text says "Choisissez la méthode d'authentification". There are two radio buttons: "Authentification Microsoft Windows" (unselected) and "Authentification SQL Server" (selected). Below the radio buttons, there is a paragraph: "Choisissez le mode de sécurité (méthode d'authentification) à utiliser pour se connecter Microsoft SQL Server 2000. En sélectionnant l'Authentification SQL Server, vous devez saisir le compte et confirmer le mot de passe." Below this text are three input fields: "Compte :" with the value "user", "Mot de passe :" with masked characters "XXXXXXXX", and "Confirmer le mot de passe :" with masked characters "XXXXXXXX". At the bottom right, there are three buttons: "< Précédent", "Suivant >", and "Annuler".

Illustration 9. Mode d'authentification sur le serveur SQL

Indiquez le compte et le mot de passe pour le serveur MySQL (cf. ill. 10).



Assistant d'installation - Kaspersky Administration Kit

Authentification SQL

Choisissez la méthode d'authentification

Choisissez la méthode d'authentification MySQL Server, indiquez le compte et confirmez le mot de passe.

Compte :

Mot de passe :

Confirmer le mot de passe :

< Précédent Suivant> Annuler

Illustration 10. Mode d'authentification sur le serveur MySQL

10. Si vous installez le serveur d'administration, définissez le chemin vers le dossier partagé (cf. ill. 11) qui sera utilisé pour entreposer :
- Les fichiers requis pour l'installation à distance d'applications Kaspersky Lab. Les fichiers sont recopiés dans le serveur d'administration lorsque vous créez les paquets d'installation.
 - Les mises à jour recopiées sur le serveur d'administration à partir de la source de mise à jour.

Des droits de lecture sur ce dossier seront accordés à tous les utilisateurs.

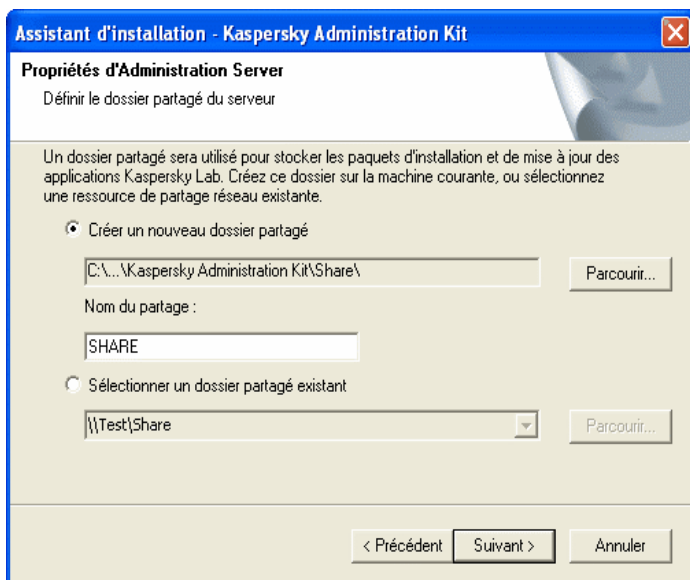


Illustration 11. Création d'un dossier partagé

Vous avez le choix entre :

- **Créer un nouveau dossier partagé** – Pour créer un nouveau dossier. Saisissez le chemin d'accès dans le champ situé en dessous.
- **Sélectionner un dossier partagé existant** – Sélectionne un dossier partagé parmi les dossiers existants.

Le dossier partagé peut se trouver sur n'importe quel ordinateur local ou distant du réseau de l'entreprise. Sélectionnez le dossier partagé à l'aide du bouton **Parcourir** ou introduisez manuellement le chemin UNC dans le champ correspondant (par exemple, \\serveur\KLShare).

Le dossier local **KLShare** est créé par défaut dans le répertoire défini pour l'installation des composants logiciels de Kaspersky Administration Kit.

11. Dans la fenêtre suivante de l'assistant, spécifiez l'adresse du serveur d'administration (cf. ill. 12):
 - Utilisez cette option lorsque le réseau dispose d'un serveur DNS et que celui-ci permet aux postes clients d'obtenir l'adresse du serveur d'administration.

- Utilisez cette option lorsque les postes clients reçoivent l'adresse du serveur d'administration par le biais du protocole NetBIOS ou que le réseau dispose d'un serveur WINS.
- Utilisez cette option lorsque l'adresse IP du serveur d'administration est statique et qu'elle ne sera pas modifiée ultérieurement.

Le cas échéant, cochez la case **Permettre service du nom NetBIOS en Anti-hacker**. Si cette option est sélectionnée, le port UDP 137, utilisé pour la réception de l'adresse IP du serveur d'administration, sera ouvert dans le dispositif anti-piratage de Kaspersky Anti-Virus 6.0 installé sur l'ordinateur.

Assistant d'installation - Kaspersky Administration Kit

Adresse du Serveur d'Administration
Définir l'adresse du Serveur d'Administration

Saisir adresse du serveur comme.

a. Nom DNS. Il est utilisé si un serveur DNS est présent et les ordinateurs clients peuvent obtenir une adresse de serveur client à travers celui-ci

b. Nom NetBIOS. Il est utilisé si les ordinateurs clients obtiennent l'adresse à travers un serveur NetBIOS, ou si un serveur WINS est présent.

c. Adresse IP. Elle est utilisée si le serveur a une adresse IP fixe qui ne sera pas modifiée par la suite.

☒ Permettre service du nom NetBIOS en Anti-hacker

< Précédent Suivant > Annuler

Illustration 12. Adresse du serveur d'administration

12. Définissez les paramètres de port pour la connexion au serveur d'administration (cf. Illustration 12.):

- Le numéro du port utilisé pour établir la connexion au serveur d'administration. Le port par défaut est **14000**. Modifiez ce numéro si ce port est déjà en service.
- Le numéro du port SSL utilisé pour la connexion sécurisée au serveur d'administration. Il s'agit par défaut du port **13000**.

Si le serveur d'administration est exploité sous Windows XP SP2, le pare-feu incorporé verrouillera les ports TCP 13000 et 14000. Vous devez donc ouvrir manuellement ces ports pour garantir l'accès à l'ordinateur sur lequel est installé le serveur d'administration.

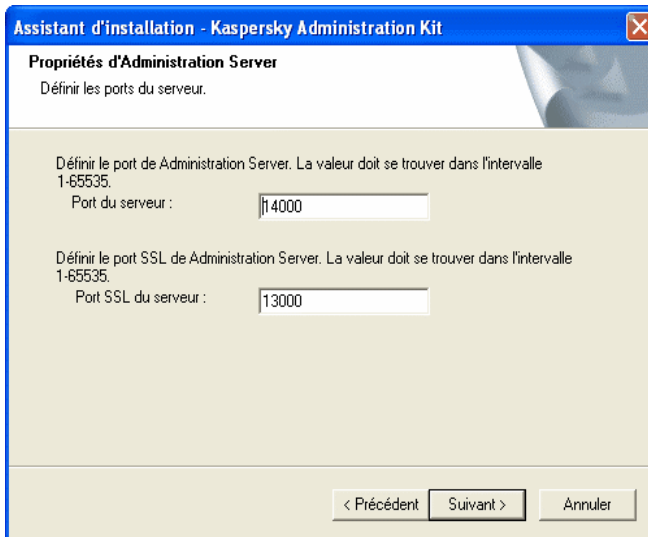


Illustration 13. Paramètres de connexion au serveur d'administration

13. Cette fenêtre de l'Assistant (cf. ill. 14) vous permet de définir le mode de création du certificat d'authentification du serveur d'administration installé.

Vous avez le choix entre :

- **Créer un nouveau certificat** : sélectionnez cette option si vous installez un nouveau serveur d'administration. Afin qu'il soit plus facile à l'avenir de restaurer les données et la structure du réseau logique de ce serveur, gardez une copie de sauvegarde du certificat. Pour ce faire, cochez la case **Créer une copie de sauvegarde du certificat**.
- **Restaurer le certificat**: sélectionnez cette option si vous restaurez le serveur d'administration sans copie de sauvegarde. Il sera possible dans ce cas de restaurer les données et la configuration du réseau logique du serveur antérieur.

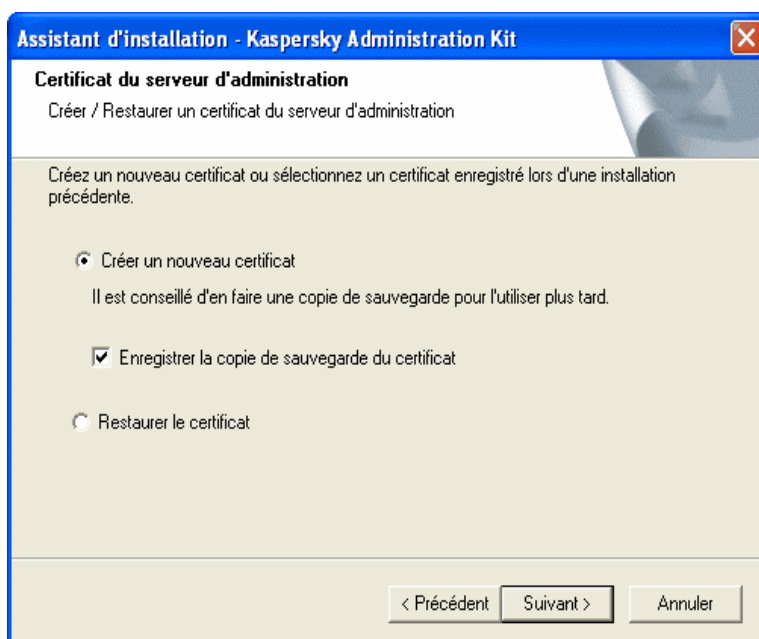


Illustration 14. Sélection du mode d'obtention du certificat du serveur d'administration

14. Si vous avez choisi la création d'un nouveau certificat à l'étape précédente et décidé de conserver sa copie de sauvegarde dans cette fenêtre (cf. ill. 15) indiquez :

- Le répertoire de stockage de la copie de sauvegarde du fichier du certificat ;
- Le mot de passe utilisé pour le chiffrement lors de la création du certificat et pour le déchiffrement lors de la restauration au départ de la copie de sauvegarde ;
- La confirmation du mot de passe

La restauration complète des données du serveur d'administration à l'avenir impose la conservation du certificat du serveur.

Lors de la restauration du certificat, il convient de saisir le mot de passe utilisé lors de la création de la copie de sauvegarde. Si le mot de passe est incorrect, la restauration du certificat échouera.

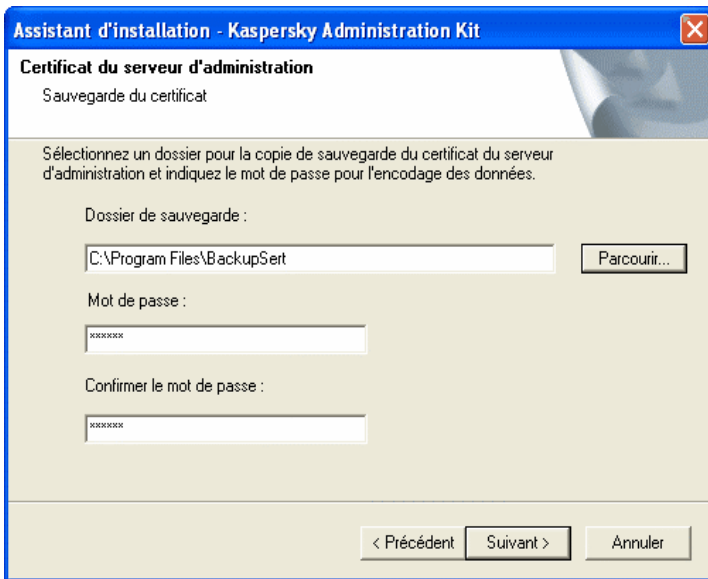


Illustration 15. Sélection du répertoire de stockage de la copie de sauvegarde du certificat

Si vous avez choisi à l'étape précédente de restaurer le certificat au départ de la copie de sauvegarde, indiquez dans cette fenêtre (cf. ill. 16) :

- Le répertoire de stockage de la copie de sauvegarde du fichier du certificat ;
- Le mot de passe qui sera utilisé pour le chiffrement lors de la création de la copie de sauvegarde du certificat.

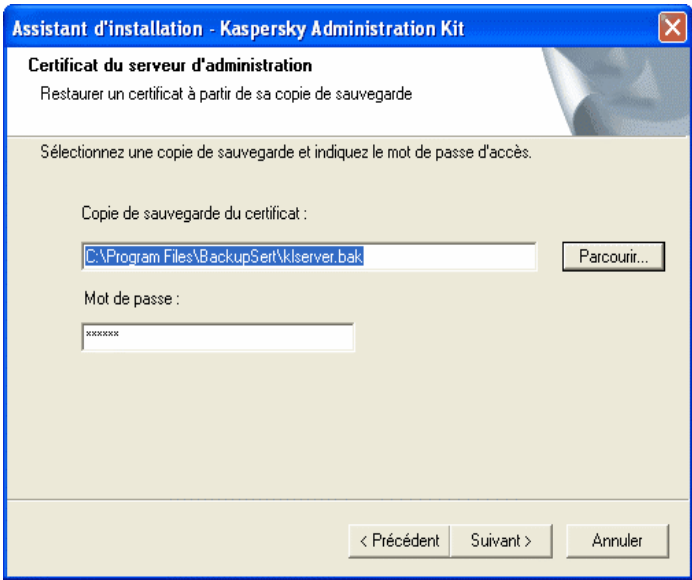


Illustration 16. Sélection du répertoire de stockage de la copie de sauvegarde du certificat

Une fois que les paramètres d'installation des composants de Kaspersky Administration Kit auront été définis, vous pouvez les vérifier et lancer l'installation.

Suite à l'installation de la console d'administration, son icône apparaît dans le menu **Démarrer → Programmes → Kaspersky Administration Kit**.

Le serveur d'administration et l'agent réseau seront installés sur l'ordinateur en qualité de service avec les attributs du tableau 2. Ce tableau présente également les attributs du service Posture Validation Server (PVS) Kaspersky Lab pour Cisco NAC, qui ne s'exécutera sur l'ordinateur que si le composant correspondant a été installé avec le serveur d'administration.

Tableau 2

Attribut	Serveur d'administration	PVS Kaspersky Lab pour Cisco NAC	Agent réseau
Nom du service	CSAdminServer	nacservernacserve r	klnagentklnage nt

Nom du service affiché	Kaspersky Administration Server	Kaspersky Lab Cisco NAC Posture Validation Server	Kaspersky Network Agent
Nom du processus dans le gestionnaire des tâches Windows	klserver.exe	klnacserver.exe klnacserver.exe	klagent.exe klagent.exe
Type de démarrage	Automatique au démarrage du système d'exploitation		
Compte	Compte système local ou compte défini par l'utilisateur (voir section 6 à la page 22).		

En plus du serveur d'administration, la version serveur de l'agent réseau sera installée sur l'ordinateur. Il fait partie du serveur d'administration et est installé et supprimé en même temps que lui. Il peut uniquement interagir avec une version du serveur d'administration installée localement. Il n'est pas nécessaire de configurer la connexion de l'agent au serveur d'administration car elle est définie par le programme en tenant compte des composants installés sur l'ordinateur. Ces paramètres ne seront pas accessibles également dans les paramètres locaux de l'agent réseau sur cet ordinateur. Cette configuration permet d'éviter les configurations complémentaires et les conflits potentiels dans le fonctionnement des composants lors d'une installation individuelle.

La version serveur de l'agent réseau est installée avec les mêmes attributs et exécuter les mêmes fonctions d'administration des applications que la version standard (cf. point 4.1.3, p. 46). Il sera soumis à la politique du groupe auquel l'ordinateur du serveur d'administration appartient en tant que client et toutes les tâches créées et exécutées pour l'agent seront possibles à l'exception des tâches liées au changement de serveur.

Il n'est pas nécessaire d'installer l'agent réseau sur l'ordinateur du serveur d'administration. Ses fonctions sont remplies par la version serveur de l'agent.

Vous pouvez consulter les propriétés des services **Kaspersky Administration Server**, **Kaspersky Network Agent** et **Kaspersky Lab Cisco NAC Posture Validation Server** et suivre leur travail à l'aide des outils d'administration standard de **Windows Gestion de l'ordinateur → Services**. Les informations relatives au service **Kaspersky Administration Server** sont consignées dans le rapport système de Windows où le serveur d'administration est installé, dans la branche **Kaspersky Event Log**.

Les groupes d'utilisateurs locaux **KLAdmins** et **KLOperators** sont créés sur le même ordinateur d'installation du serveur d'administration. Si le serveur d'administration est configuré pour fonctionner sous un compte d'utilisateur de domaine, les groupes **KLAdmins** et **KLOperators** sont ajoutés à la liste de groupes d'utilisateurs du domaine. Les groupes peuvent être modifiés à l'aide des outils standard d'administration de Windows.

3.3. Désinstallation des composants de Kaspersky Administration Kit

Pour désinstaller Kaspersky Administration Kit, vous pouvez utiliser la commande **Désinstaller Kaspersky Administration Kit** du menu **Démarrer => Tous les programmes => Kaspersky Administration Kit** ou les outils standard Windows pour l'installation et la suppression d'applications. Après l'exécution de l'assistant, tous les composants applicatifs (y compris les plug-ins) seront supprimés de l'ordinateur. Si vous avez choisi dans l'assistant de ne pas supprimer le dossier partagé (**KLShare**), supprimez-le manuellement une fois que celui-ci ne sera plus nécessaire.

Au moment de la suppression, vous aurez la possibilité de conserver une copie de sauvegarde de l'agent réseau.

3.4. Mise à jour vers une version plus récente de l'application

Pour passer de la version 4.x (Service Pack 1) ou 5.x (Service Pack 2) à une version ultérieure de Kaspersky Administration Kit, supprimez la version précédente et installez la nouvelle en suivant les instructions données dans ce document.

Si vous faites une mise à jour de la version 5.0 (Service Pack 3) ou 6.0 vers une nouvelle version, les données de sauvegarde les plus récentes de l'ancienne version de l'application sont restaurées. Nous vous recommandons de suivre la procédure suivante :

1. Créez une copie de sauvegarde des données du serveur d'administration à l'aide de l'outil **klbackup.exe**. Cet outil est fourni avec le paquet de distribution Kaspersky Administration Kit et se trouve dans le dossier racine d'installation du serveur d'administration. Notez que pour restaurer complètement les données du serveur d'administration,

vous devez faire une copie de sauvegarde du certificat serveur. Ce paramètre est obligatoire pour l'outil **klbackup.exe**.

2. Lancez l'installation de la version la plus récente de Kaspersky Administration Kit 6.0 sur l'ordinateur où se trouve installée la version antérieure du serveur d'administration et/ou de la console. Mettez à jour le composant. Au cours de la mise à jour, toutes les données et tous les paramètres de la version précédente du serveur d'administration et/ou de la console sont enregistrées et rendues disponibles dans la nouvelle version. La compatibilité descendante est assurée entre la nouvelle et l'ancienne version du serveur d'administration.
3. Afin de pouvoir mettre à niveau l'agent réseau installé sur les ordinateurs du réseau, créez un groupe ou une tâche d'installation globale de la nouvelle version du composant. Exécutez la tâche manuellement ou planifiée. Une fois la tâche terminée, l'agent réseau aura été mis à niveau avec la nouvelle version.

En cas de problème lors de l'installation, vous pouvez restaurer la version antérieure de Kaspersky Administration Kit à l'aide de la copie de sauvegarde du serveur d'administration créée avant la mise à jour.

Si plusieurs serveurs d'administration sont installés, la mise à jour des serveurs peut être effectuée à l'aide d'une tâche d'installation à distance utilisant le paquet d'installation du serveur d'administration (voir section 4.1.4 à la page 41)

CHAPITRE 4. INSTALLATION ET DÉSINSTALLATION D'APPLICATIONS SUR DES POSTES CLIENTS

Avant de procéder à l'installation, assurez-vous que les postes clients répondent aux spécifications matérielles et logicielles (voir section 1.3 à la page 9).

Kaspersky Administration Kit permet l'installation et la désinstallation d'applications Kaspersky Lab sur les postes clients du réseau logique par les procédés suivants :

- la méthode centralisée ou à distance à travers la console d'administration;
- l'installation locale, sur chaque poste client.

Le composant Agent Réseau assure la connectivité entre le serveur d'administration et les postes clients. Par conséquent, il faut l'installer sur chaque ordinateur connecté au système d'administration distant, avant même d'installer les applications antivirus. Lors d'une installation centralisée via la console d'administration, l'agent doit être installé en même temps qu'une des applications.

Sur l'ordinateur où est installé le serveur d'administration, seule la version serveur de l'agent peut remplir le rôle de l'agent. Il fait partie du serveur d'administration et est installé ou supprimé en même temps que lui (cf. point 3.2, p. 18).

Il n'est pas nécessaire d'installer l'agent réseau sur cet ordinateur.

Le composant Agent Réseau est installé de la même manière que les applications antivirus. Il peut être installé à distance ou localement.

Les agents d'administration peuvent varier en fonction de l'application de Kaspersky Lab pour laquelle ils ont été développés. Dans certains cas, seule l'installation locale de l'agent réseau est possible. Pour obtenir de plus amples informations, consultez les guides des applications concernées. L'agent réseau est installé sur le poste une seule fois.

Les plug-ins de console fournissent l'interface de gestion de Kaspersky Administration Kit. Pour utiliser cette interface de gestion, le plug-in correspondant doit être installé sur le poste administrateur. Lors du déploiement d'une application, le plug-in est installé automatiquement avec la création du premier paquet d'installation de l'application. En cas d'installation locale, le plug-in est installé manuellement par l'administrateur.

La version actuelle de Kaspersky Administration Kit permet d'administrer à distance les applications Kaspersky Lab suivantes :

- protection pour les stations de travail et serveurs de fichiers :
 - Kaspersky Anti-Virus 5.0 for Windows File Servers;
 - Kaspersky Anti-Virus 6.0 for Windows Servers;
 - Kaspersky Anti-Virus 5.0 for Windows Workstations;
 - Kaspersky Anti-Virus 6.0 for Windows Workstations;
 - Kaspersky Anti-Virus 6.0 Second Opinion Solution;
 - Kaspersky Anti-Virus 5.7 for Novell NetWare;
- protection du périmètre informatique :
 - Kaspersky Anti-Virus 5.6 for Microsoft ISA Server 2000 Enterprise Edition.
- protection pour systèmes de messagerie :
 - Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2000/2003, Service Pack 1;
 - Kaspersky Anti-Virus 5.5 for Microsoft Exchange Server 2003, Service Pack 1.

Pour de plus amples informations sur les applications informatiques administrables par Kaspersky Administration Kit, consultez le manuel de l'application.

4.1. Installation à distance du logiciel

L'installation à distance peut être réalisée depuis le poste de travail de l'administrateur dans la fenêtre principale de Kaspersky Administration Kit.

Certaines applications de Kaspersky Lab peuvent uniquement être installées localement sur les postes client (pour de plus amples informations, consultez les guides des applications concernées). L'administration à distance de ces applications via Kaspersky Administration Kit est possible.

Pour installer une application à distance :

1. Créez un paquet d'installation (cf. point 4.1.1, p.40). Il doit contenir les fichiers indispensables à l'installation ainsi qu'un fichier reprenant la description du paquet d'installation en question.
2. Créez une tâche d'installation à distance (cf. point 4.1.7, p. 55).

Il convient d'installer une tâche globale d'installation à distance pour installer l'application sur tous les ordinateurs du réseau logique ou sur quelques groupes d'administration ou sur des ordinateurs de différents groupes.

Pour installer l'application sur tous les postes clients de n'importe quel groupe d'administration (tous les groupes intégrés et les serveurs secondaires), il faut créer une tâche de groupe d'installation à distance.

Vous pouvez utiliser l'assistant d'installation à distance afin de créer la tâche de groupe (cf. point 4.2, p. 73) ou la tâche globale.

La tâche ainsi créée sera exécutée selon l'horaire défini. Les paramètres de fonctionnement de l'application sur chaque poste client sont définis conformément à la stratégie du groupe et aux paramètres de cette application par défaut.

Vous pouvez interrompre l'installation en interrompant manuellement la tâche.

Tous les paquets d'installation créés pour le serveur d'administration sont placés sous l'entrée **Installation distante** de l'arborescence de console. Vous pouvez examiner les propriétés et changer le nom ou les paramètres du paquet d'installation. Les paquets d'installation sont entreposés sur le serveur d'administration dans le dossier **Packages**, dans un dossier partagé spécifié.

Vous pouvez consulter les propriétés du paquet d'installation, modifier son nom ou sa configuration dans la boîte de dialogue **Propriétés: <Nom du paquet >** (cf. ill. 20). Cette fenêtre s'ouvre à l'aide de la commande **Propriétés** du menu contextuel ou de l'élément équivalent dans le menu **Action**.

Les paquets d'installation créés peuvent être diffusés sur les serveurs d'administration secondaires (cf. point 4.1.5, p. 50) ou sur les ordinateurs du groupe à l'aide des agents de mise à jour (cf. point 4.1.6, p. 52)

Un seul paquet d'installation peut être utilisé plusieurs fois pour créer des tâches d'installation à distance.

L'installation de l'application peut également être effectuée en mode non-interactif (pour de plus amples détails, voir section 4.3.3 à la page 44).

4.1.1. Création d'un paquet d'installation

Pour créer un paquet d'installation :

1. Connectez-vous au serveur d'administration souhaité.
2. Dans l'arborescence de console, sélectionnez l'entrée **Installation distante**, ouvrez le menu contextuel et cliquez sur **Nouveau / Paquet** (cette commande se trouve également sous le menu **Action**) pour lancer un **Assistant**. Cette action entraîne le lancement de l'Assistant. Suivez les instructions qui s'affichent.
3. Indiquez le nom du paquet d'installation. A l'étape suivante, vous pourrez désigner les applications à installer (cf. ill. 17).

Si vous installez une application qui peut être installée à distance via Kaspersky Administration Kit, sélectionnez une des options suivantes dans la liste déroulante : **Générer le paquet d'application Kaspersky Lab**. A l'aide du bouton **Parcourir**, sélectionnez le fichier de description de l'application (fichier **.kpd** faisant partie des fichiers d'installation de toutes les applications Kaspersky Lab pouvant être administrées à distance à l'aide de Kaspersky Administration Kit) ou l'archive auto-extractible de l'application de Kaspersky Lab (fichier **.exe** téléchargeable depuis le site de Kaspersky Lab). Les champs du nom de l'application et de sa version sont remplis automatiquement.

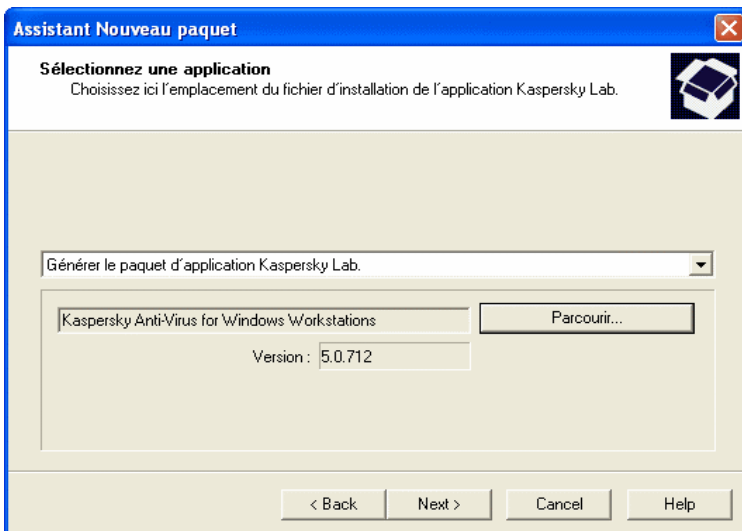


Illustration 17. Création d'un paquet d'installation. Sélection de l'application à installer

Les paramètres du paquet d'installation sont définis par défaut et correspondent à ceux de l'application à installer. Vous pourrez les modifier après la création du paquet dans la fenêtre des propriétés (cf. point 4.1.2, p. 43).

Lors de la création d'un paquet pour l'installation d'autres applications (cf. III. 18) :

- Dans la liste déroulante, sélectionnez : **Générer le paquet d'installation du fichier exécutable spécifié** ;
- Indiquez le chemin d'accès au fichier d'installation de l'application à l'aide du bouton **Parcourir**.
- Cochez la case **Copier tout le dossier dans le paquet** si le contenu du paquet doit être identique à celui du fichier d'installation.
- Définissez les paramètres de lancement du fichier exécutable dans la ligne de saisie si cela est nécessaire pour l'installation de l'application (par exemple, lancement en mode silencieux à l'aide du commutateur **/s**).

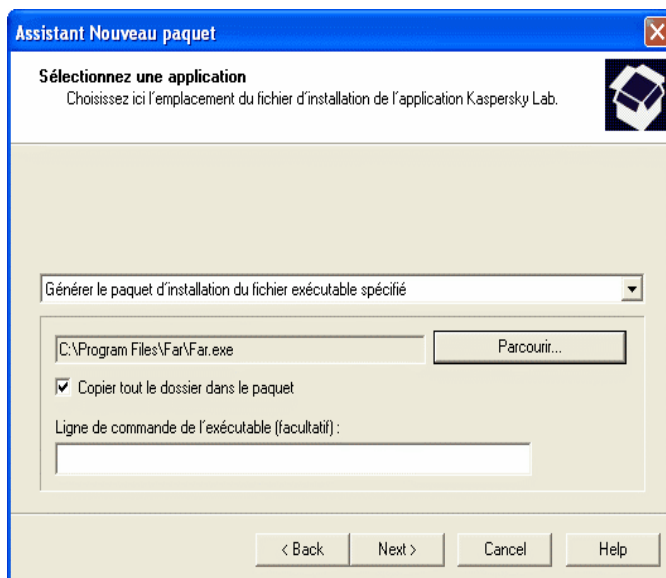


Illustration 18. Création d'un paquet d'installation pour une application indiquée par l'utilisateur

4. Dans la fenêtre suivante de l'Assistant (cf. III. 19), vous pouvez inclure une clé de licence dans le paquet d'installation en cliquant sur **Parcourir** puis en sélectionnant le fichier de licence (avec extension **.key**).

Si vous ne souhaitez pas ajouter une clé de licence au paquet d'installation, cliquez sur **Suivant**.

La clé de licence n'est pas nécessaire lors de la création du paquet d'installation du serveur d'administration et de l'agent réseau.

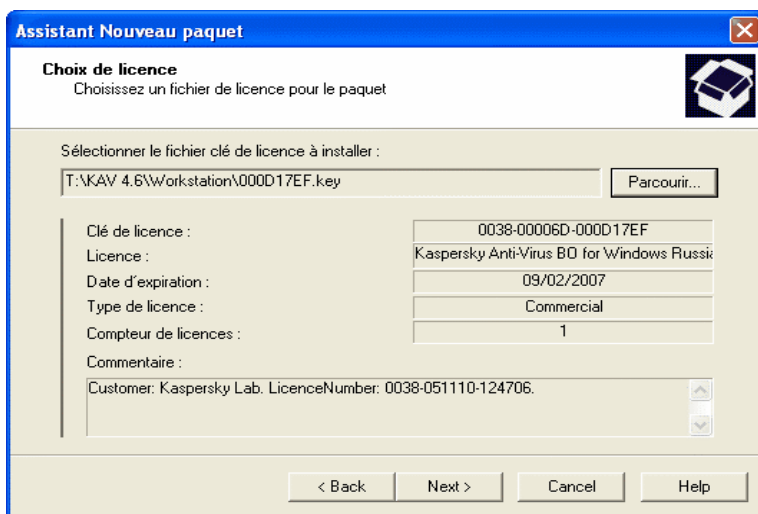


Illustration 19. Création d'un paquet d'installation. Sélection d'une clé de licence

5. Un ensemble de fichiers nécessaires pour installer l'application sur les clients est alors chargé dans le dossier partagé du serveur d'administration. Le serveur vérifie, dans le poste administrateur, la disponibilité du plug-in de console pour cette application. Si le plug-in n'a pas été installée ou si sa version est plus récente que celle de l'application, il sera respectivement installé, ou remplacé.

Après la fin de l'Assistant, un nouveau paquet d'installation sera ajouté sous l'entrée **Installation distante** et présenté dans le panneau de détails.

4.1.2. Affichage configuration des paramètres du paquet d'installation

Pour examiner les propriétés et changer le nom du paquet d'installation dans la boîte de dialogue :

déployez l'entrée **Installation distante** dans l'arborescence de console, sélectionnez le paquet d'installation requis dans le panneau de résultats et utilisez la commande **Propriétés** dans le menu contextuel ou dans le menu **Actions**.

Ceci permet d'ouvrir la boîte de dialogue **Propriétés de <Nom du paquet d'installation>** (cf. III. 20) composée des onglets suivants : **Général**, **Paramètres**, **Licences** et **Redémarrage du S.E.**.

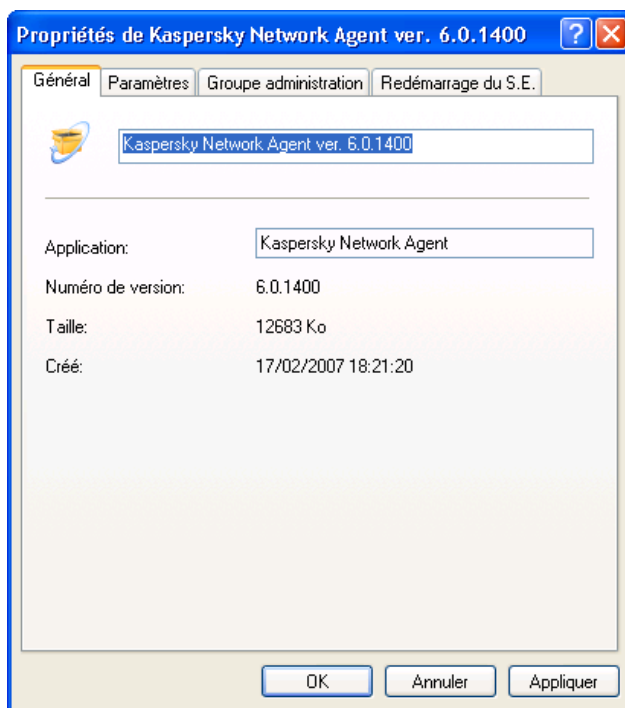


Illustration 20. Boîte de dialogue Propriétés du paquet d'installation.
L'onglet **Général**

L'onglet **Général** (cf. ill. 20) affiche des informations générales sur le paquet :

- **Application**
- **Version**
- **Taille**
- **Créé(e)**

L'onglet **Paramètres** (cf. ill. 21) affiche les paramètres du paquet d'installation, qui correspondent à ceux de l'application pour laquelle le paquet a été créé. Ce sont des paramètres par défaut, qui peuvent être modifiés si nécessaire.

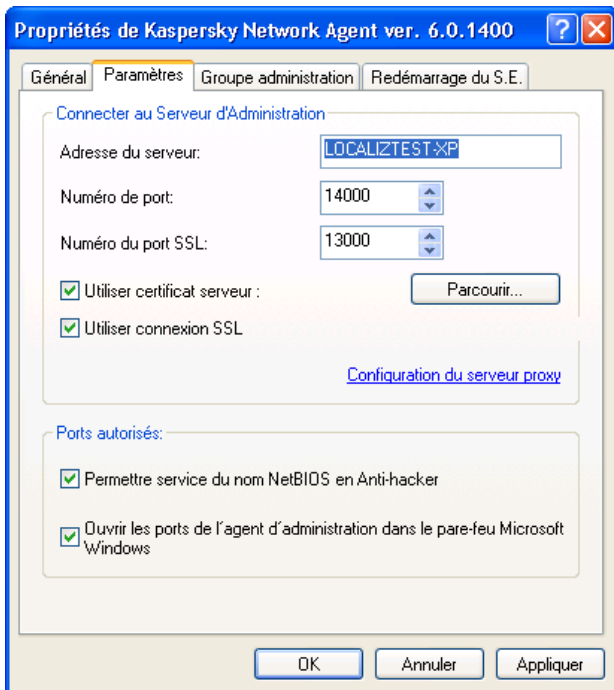


Illustration 21. Boîte de dialogue Propriétés du paquet d'installation.
L'onglet **Paramètres d'installation**

L'onglet **Infos de licence** (cf. ill. 22) présente des informations générales sur la licence de l'application contenue par le paquet.

L'onglet **Licence** ne figure pas dans les propriétés du paquet d'installation du serveur d'administration et de l'agent réseau.

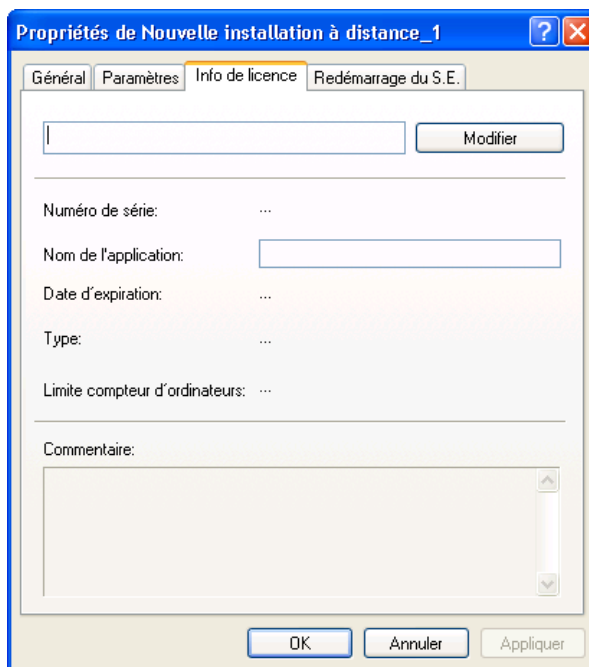


Illustration 22. Fenêtre de propriétés du paquet d'installation
Onglet **Licence**

Dans la page **Redémarrage du S.E.** (cf. ill. 23) vous pouvez définir les actions à réaliser lorsqu'il faut redémarrer l'ordinateur après l'installation de l'application:

- **Ne pas redémarrer le système d'exploitation.**
- **Si nécessaire, redémarrer le système d'exploitation automatiquement** - Le système d'exploitation n'est redémarré que si cela s'avère nécessaire.
- **Confirmer l'action auprès de l'utilisateur** – le choix de cette option permet de :
 - créer un message destiné à l'utilisateur qui sera affiché pour l'informer qu'il faut redémarrer le système d'exploitation, dans le champ associé;
 - spécifier la fréquence de la notification de redémarrage du système d'exploitation, en cochant la case **Répéter toutes les (min.)** et en spécifiant l'intervalle à utiliser pour afficher les notifications.

- configurer le redémarrage automatique du système d'exploitation si l'ordinateur ne l'a pas été manuellement dans l'intervalle de temps spécifié, à compter de l'installation de l'application. Pour ce faire, cochez la case **Redémarrage forcé après (min.)** et spécifiez l'intervalle de temps souhaité.

Si vous choisissez le redémarrage automatique de l'ordinateur, cochez la case **Fermer automatiquement les applications en cours**. Celle-ci est décochée par défaut.

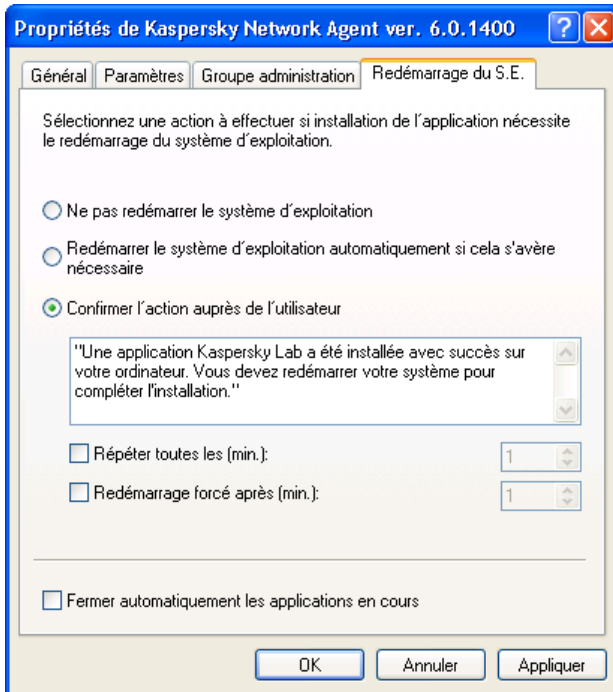


Illustration 23. Fenêtre de propriétés du paquet d'installation
Onglet **Redémarrage du S.E**

4.1.3. Création et configuration d'un paquet d'installation pour l'agent réseau

Le paquet d'installation pour l'installation à distance de l'agent réseau ne doit pas être créé manuellement. Il est créé automatiquement lors de l'installation de Kaspersky Administration Kit et se trouve sous le nœud **Installation distante**.

Si le paquet pour l'installation à distance de l'agent réseau a été supprimé, il faudra pour le recréer choisir le fichier **klagent.kpd**, situé dans le répertoire **NetAgent** du fichier de distribution de Kaspersky Administration Kit, en guise de fichier de description.

Les paramètres du paquet d'installation de l'agent réseau sont réduits au minimum indispensable pour garantir le fonctionnement du composant directement après son installation. Par défaut, les paramètres sont identiques aux paramètres de l'application. Le cas échéant, vous pouvez les modifier sur les **Paramètres** et **Groupe d'administration** de la fenêtre de consultation des propriétés du paquet d'installation.

Dans l'onglet **Paramètres** (cf. ill. 21), vous trouverez les paramètres qui définissent la connexion de l'agent réseau au serveur d'administration après son installation sur le poste client (les valeurs par défaut sont celles du serveur actuel) :

- Adresse de l'ordinateur sur lequel est installé le serveur d'administration.
- Le numéro du port utilisé pour établir la connexion non sécurisée au serveur d'administration. Par défaut, il s'agit du port **14000**. Vous pouvez en choisir un autre s'il est occupé.
- Le numéro du port utilisé pour établir la connexion non sécurisée au serveur d'administration via le protocole SSL Il s'agit par défaut du port **13000**.

Seule la notation décimale est admise.

- Le fichier du certificat pour authentifier l'accès au serveur d'administration. La valeur de ce paramètre est définie par la case **Utiliser le certificat du serveur**.

Si la case n'est pas cochée (valeur par défaut), le fichier de certificat sera obtenu directement auprès du serveur d'administration lorsque l'agent s'y connectera pour la première fois.

Si la case **Utiliser le certificat du serveur** est cochée, l'authentification aura lieu sur la base du fichier de certificat sélectionné à l'aide du bouton **Parcourir**. Ce fichier possède l'extension **.cer** et se trouve sur le serveur d'administration dans le dossier **Cert** du répertoire d'installation de Kaspersky Administration Kit. Vous pouvez modifier le fichier de certificat à l'aide du bouton **Parcourir**.

- Le port utilisé pour la connexion de l'agent réseau au serveur : simple ou sécurisé. Cette valeur est définie par la case **Utiliser connexion SSL**. Lorsque la case est cochée, la connexion s'établit via un port sécurisé grâce au protocole SSL. Si la case n'est pas cochée, la connexion n'est pas sécurisée.

- Les paramètres de connexion via le serveur proxy. Si la connexion de l'agent au serveur d'administration s'opère via un serveur proxy, cochez la case **Utiliser le serveur proxy**. Cliquez ensuite sur le bouton **Paramètres** et dans la fenêtre qui s'ouvre, saisissez l'adresse du serveur proxy, le nom d'utilisateur et le mot de passe.
- L'ouverture du port UDP 137, utilisé pour la réception de l'adresse IP du serveur d'administration, dans le dispositif anti-piratage de Kaspersky Anti-Virus 6.0. Pour ce faire, cochez la case **Permettre service du nom NetBIOS en Anti-hacker**.
- L'autorisation du port UDP, indispensable au bon fonctionnement de l'agent réseau, dans la liste des exceptions du pare-feu Microsoft Windows. Pour ce faire, cochez la case **Ouvrir les ports de l'agent réseau dans le pare-feu Microsoft Windows**.

Après l'installation de l'agent réseau, vous pouvez modifier les paramètres de connexion au serveur d'administration à l'aide de stratégies et de la configuration de l'application.

En cas de nouvelle installation à distance de l'agent réseau sur le poste client, les valeurs des paramètres de connexion au serveur et le certificat du serveur d'administration sont remplacés par de nouveaux.

Dans l'onglet **Groupe d'administration** (cf. ill. 24), définissez le sous-groupe **Réseau** où seront ajoutés les postes après l'installation de l'agent réseau. Choisissez une des options suivantes :

- Ajouter les postes au dossier **Selon la situation du poste dans le réseau Windows** : domaine ou groupe de travail (valeur choisie par défaut) ;
- Ajouter tous les postes **Dans le groupe** défini dans le champ. Si vous choisissez cette option, il faudra saisir le nom du dossier dans le champ situé en dessous. Si ce répertoire n'existe pas dans le répertoire **Réseau**, il sera créé (vous pouvez également indiquer le nom de n'importe lequel des dossiers existant dans le répertoire **Réseau**).

Ce répertoire accueillera tous les postes découverts à nouveau dans le réseau, même si ceux-ci avaient été préalablement découverts par le serveur d'administration et placés dans le dossier correspondant à leur situation dans le réseau avant l'installation de l'agent réseau.

Après l'installation de l'agent réseau, il sera impossible de modifier le dossier de placement des ordinateurs dans le groupe **Réseau**. Ce paramètre ne fait pas partie de la stratégie ou des paramètres de l'application.

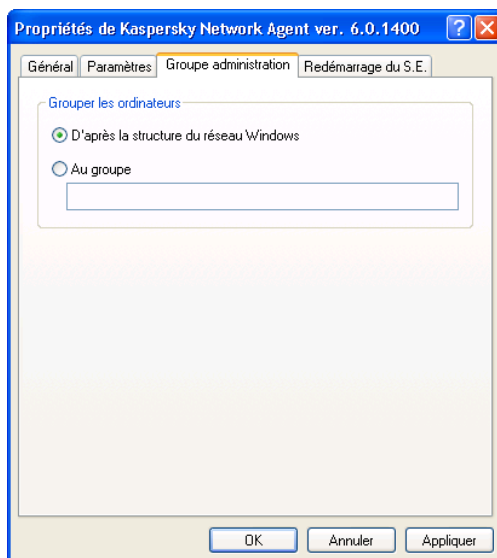


Illustration 24. Fenêtre de propriétés du paquet d'installation. Onglet **Groupe d'administration**

L'agent réseau sera installé sur l'ordinateur en qualité de service avec les attributs suivants :

- Nom du service (**KLNAgent**) ;
- Nom désigné **Kaspersky Network Agent**.
- Lancement automatique au démarrage du système d'exploitation ;
- Compte **Système local**

Vous pouvez consulter les propriétés du service **Kaspersky Network Agent** et suivre ou arrêter son travail à l'aide des outils d'administration standard de **Windows Gestion de l'ordinateur / Services**.

4.1.4. Création et configuration d'un paquet d'installation pour le serveur d'administration.

Lors de la création d'un paquet d'installation pour le serveur d'administration, sélectionnez le fichier de définition **ak6.kpd** situé dans la racine du répertoire d'installation de Kaspersky Administration Kit.

Les paramètres du paquet d'installation sont répartis dans deux onglets : **Général** (cf. ill. 20) et **Redémarrage du S.E.** (cf. ill 23). Les autres paramètres sont les paramètres par défaut du serveur d'administration.

4.1.5. Création d'une tâche de diffusion du paquet d'installation sur les serveurs d'administration secondaires

Afin de créer une tâche de diffusion du paquet d'installation sur les serveurs d'administration secondaires :

1. Connectez-vous au serveur d'administration souhaité.
2. Sélectionnez le nœud **Tâches globales** dans l'arborescence de la console, affichez le menu contextuel et sélectionnez le point **Nouveau→Tâche** ou choisissez l'élément équivalent du menu **Action**. Cette action entraîne le lancement de l'Assistant. Suivez les instructions qui s'affichent.
3. Pour l'application Kaspersky Administration Kit, sélectionnez le type de tâche **Diffusion du paquet d'installation**.
4. Dans la fenêtre suivante (cf. ill. 25), sélectionnez les types de paquets qu'il faut diffuser. Choisissez l'une des deux options :
 - **Tous les paquets d'installation.**
 - **Uniquement les paquets d'installation sélectionnés.** Dans ce cas, cochez la case en regard des paquets d'installation requis.

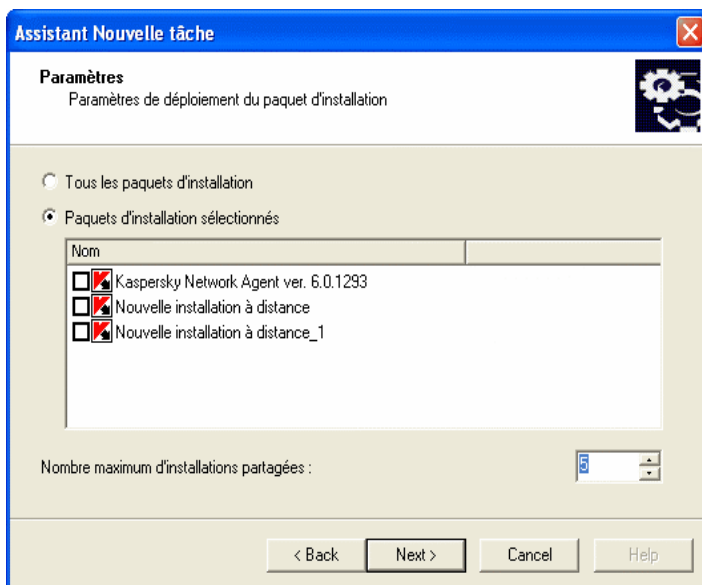


Illustration 25. Sélection des paquets d'installation

Indiquez la valeur souhaitée dans le champ **Nombre maximum de redémarrages simultanés**.

5. Dans la fenêtre suivante de l'assistant (cf. ill. 26), cochez les cases en regard des serveurs d'administration secondaires sur lesquels il faut diffuser les paquets d'installation.

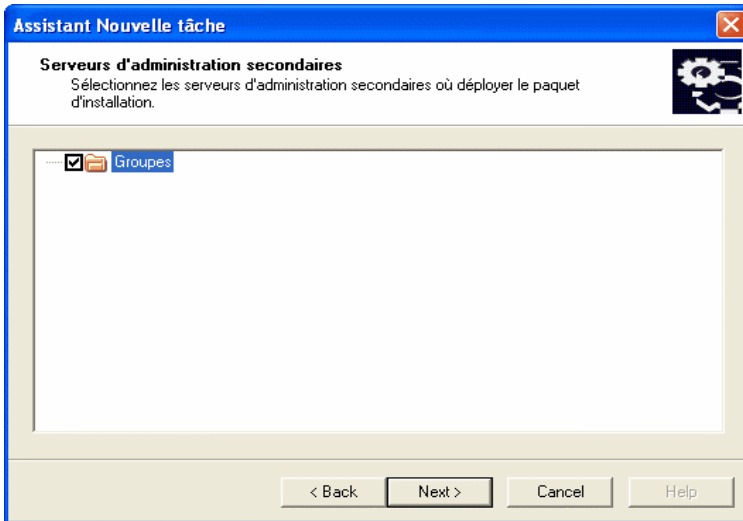


Illustration 26. Sélection des serveurs d'administration secondaires

6. Définissez ensuite le compte sous lequel la tâche sera lancée sur les postes (pour de plus amples informations, consultez le point 4.1.7 à la page 55).
7. Pour quitter l'Assistant, cliquez sur **Terminer**.

4.1.6. Diffusion des paquets d'installation dans les limites du groupe à l'aide d'agents d'administration

Les agents de mise à jour peuvent intervenir dans la diffusion de paquets d'installation dans les limites du groupe. Les agents de mise à jour obtiennent les paquets d'installation et les mises à jour du serveur d'administration et les conservent dans le répertoire d'installation de l'application de Kaspersky Lab.

Il est impossible de changer l'emplacement du répertoire contenant les mises à jour et les paquets d'installation ou de limiter sa capacité.

Les paquets d'installation seront ensuite diffusés via une diffusion multi-adresse vers les postes clients. La diffusion de nouveaux paquets d'installation dans les limites du groupe se produit une fois. Si le poste n'était pas connecté au réseau logique au moment de la diffusion, le paquet d'installation indispensable sera

téléchargé automatique de l'agent de mise à jour lors du lancement de la tâche d'installation de l'agent réseau.

Pour constituer la liste des agents de mise à jour et les configurer pour la diffusion de paquets d'installation sur les postes du groupe :

1. Connectez-vous au serveur d'administration souhaité.
2. Sélectionnez le groupe dans l'arborescence de la console puis, ouvrez le menu contextuel afin de choisir le point **Propriétés** ou sélectionnez l'élément équivalent dans le menu **Action**.
3. Dans la fenêtre des propriétés qui s'ouvre, composez la liste des postes qui rempliront le rôle d'agent de mise à jour dans les limites du groupe à l'aide des boutons **Ajouter** et Supprimer de l'onglet **Agents de mise à jour** (cf. Ill. 27).

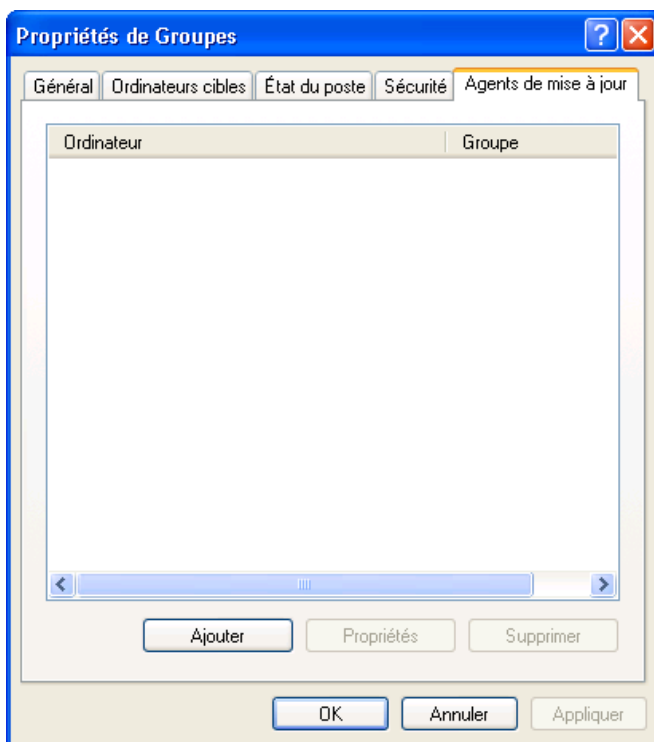


Illustration 27. Fenêtre des propriétés du groupe.
Onglet **Agents de mise à jour**

4. Modifiez les paramètres de l'agent de mise à jour. Pour ce faire, sélectionnez l'agent dans la liste puis, cliquez sur **Propriétés**. Dans la fenêtre **<Nom de l'agent de mise à jour> propriétés** (cf. ill. 28) qui s'ouvre :
 - Indiquez le numéro du port utilisé pour la connexion du poste client à l'agent de mise à jour. Par défaut, il s'agit du port **14001**. Vous pouvez en choisir un autre s'il est occupé.
 - Indiquez le numéro du port utilisé pour la connexion sécurisée du poste client à l'agent de mise à jour via le protocole SSL. Il s'agit par défaut du port **13001**.
 - Cochez la case **Utiliser la diffusion multi-adresse** et remplissez les champs **IP de multidiffusion** et **Numéro de port d'IP-MULTICAST**.
5. Cliquez sur **Appliquer** ou **OK**.

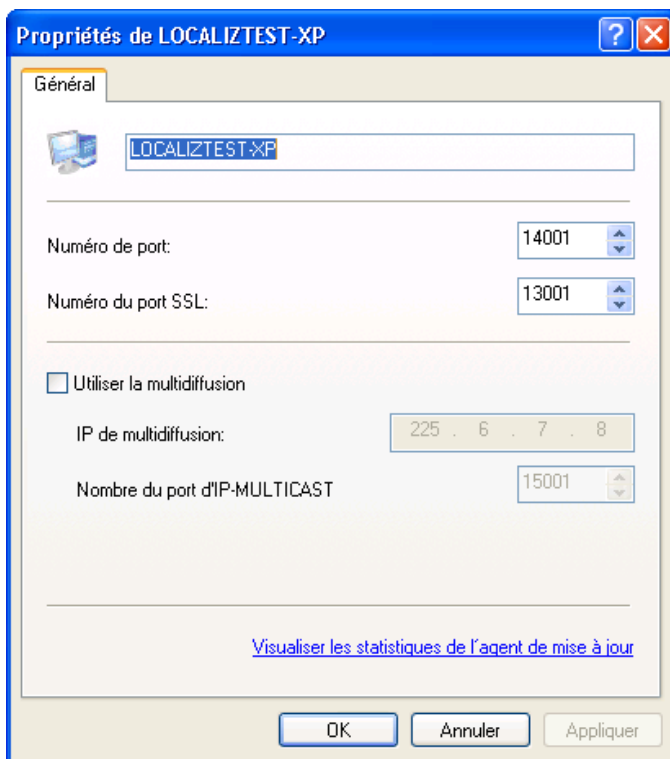


Illustration 28. Fenêtre des propriétés de l'agent de mise à jour

4.1.7. Création d'une tâche d'installation à distance

Deux méthodes permettent d'effectuer le déploiement d'applications sur les postes clients : **l'installation par envoi** et **l'installation à l'aide d'un script de connexion**.

L'installation par envoi permet d'installer à distance des applications sur des postes clients spécifiques de votre réseau logique. Lors de l'exécution de la tâche de déploiement d'une application, le serveur d'administration recopie ses fichiers d'installation depuis le dossier partagé vers les dossiers temporaires de chaque poste client, puis exécute le programme d'installation sur ces ordinateurs. Pour forcer l'installation d'une application, le serveur d'administration doit posséder les privilèges nécessaires pour lancer à distance les applications sur les clients du réseau logique. Cette méthode est recommandée pour l'installation d'applications sur des ordinateurs sous MS Windows NT/2000/2003/XP qui prennent en charge cette caractéristique, ou sur des ordinateurs sous MS Windows 98/Me, sur lesquels Agent Réseau est installé.

Si le serveur d'administration et un client communiquent entre eux par Internet, ou si la connexion est protégée par un pare-feu, il n'est pas possible d'utiliser de dossiers partagés pour transférer des données. Dans ce cas, l'agent réseau peut être utilisé pour l'installation des fichiers sur le client. L'agent réseau doit être installé en local sur ces ordinateurs.

L'installation avec un script de connexion vous permet de lancer le déploiement d'applications dès qu'un utilisateur spécifique ouvre une session sur le domaine (plusieurs utilisateurs). Suite à l'exécution de la tâche, le lancement du programme d'installation situé dans le dossier partagé du serveur d'administration est consigné dans le script de lancement pour les utilisateurs défini. Le programme d'installation d'application est entreposé dans le dossier partagé du serveur d'administration. Pour garantir la réussite d'une tâche de déploiement d'application, le compte utilisateur ou le serveur d'administration doit posséder des privilèges de modification des scripts de connexion dans la base de données du contrôleur de domaine. L'administrateur de domaine possède un tel privilège, autrement dit cette tâche ou tout le serveur d'administration doit être lancée avec les privilèges de cet utilisateur. Quand un utilisateur spécifié ouvre une session sur le domaine, l'installation démarre sur le poste client utilisé pour se connecter. Cette méthode est recommandée pour installer des applications Kaspersky Lab sur des ordinateurs sous MS Windows 95/98/Me.

Pour que la tâche d'installation à distance à l'aide du scénario de lancement réussisse, les utilisateurs pour lesquels le script est modifié doivent jouir des privilèges d'administrateur sur l'ordinateur local.

Les tâches de groupe d'installation à distance de l'application sur les postes client sont exécutées uniquement selon la méthode de l'installation par envoi. Lors de la création d'une tâche globale, vous pouvez choisir la méthode qui vous convient : installation par envoi ou installation avec un script de connexion.

Pour créer une tâche globale d'installation à distance selon la méthode d'installation par envoi :

1. Connectez-vous au serveur d'administration souhaité.
2. Sélectionnez le nœud **Tâches globales** dans l'arborescence de la console, affichez le menu contextuel et sélectionnez le point **Nouveau/Tâche** ou choisissez l'élément équivalent du menu **Action**. Cette action entraîne le lancement de l'Assistant de création de tâche. Suivez les instructions qui s'affichent.
3. Définissez le nom de la tâche.
4. Lors de la sélection de l'application et de la définition du type de tâche (cf.ill. 29), sélectionnez les valeurs **Kaspersky Administration Kit** et **Installation distante de l'application**.

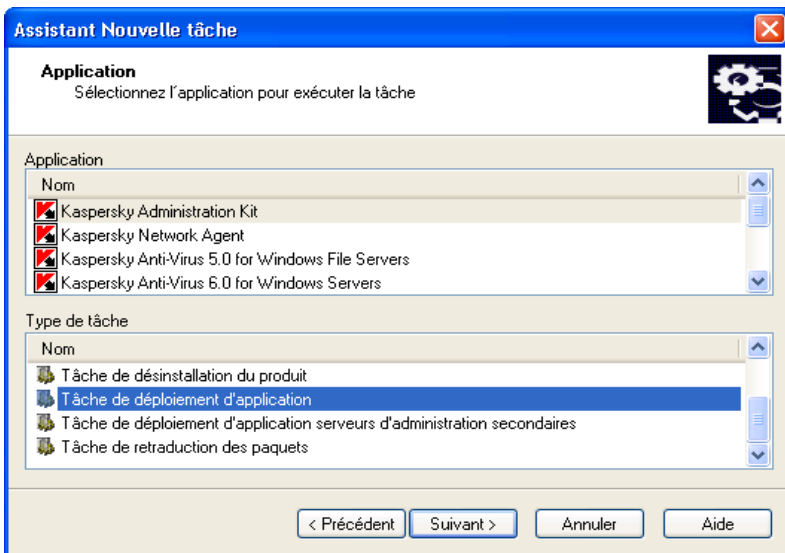


Illustration 29. Définition du type de tâche

5. Précisez ensuite le paquet d'installation qui sera installé dans le cadre de l'exécution de cette tâche (cf. ill. 30). Sélectionnez le paquet parmi les paquets créés pour ce serveur d'administration ou créez-en un nouveau à l'aide du bouton **Nouveau**.

Certaines applications administrées à l'aide de Kaspersky Administration Kit peuvent être installées uniquement localement. Pour obtenir de plus amples informations, consultez les guides des applications correspondantes.

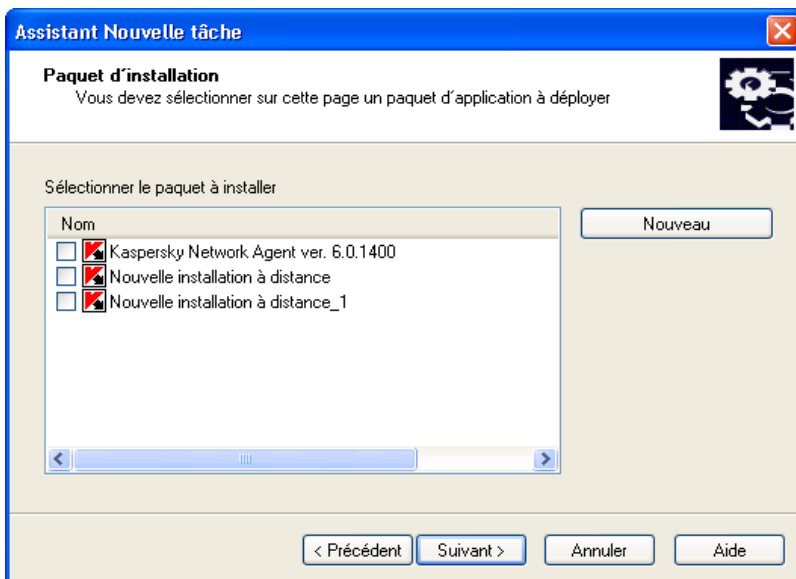


Illustration 30. Sélection du paquet d'installation à installer

6. Sélectionnez à cette étape l'option **Installation par envoi** (cf. ill. 31).

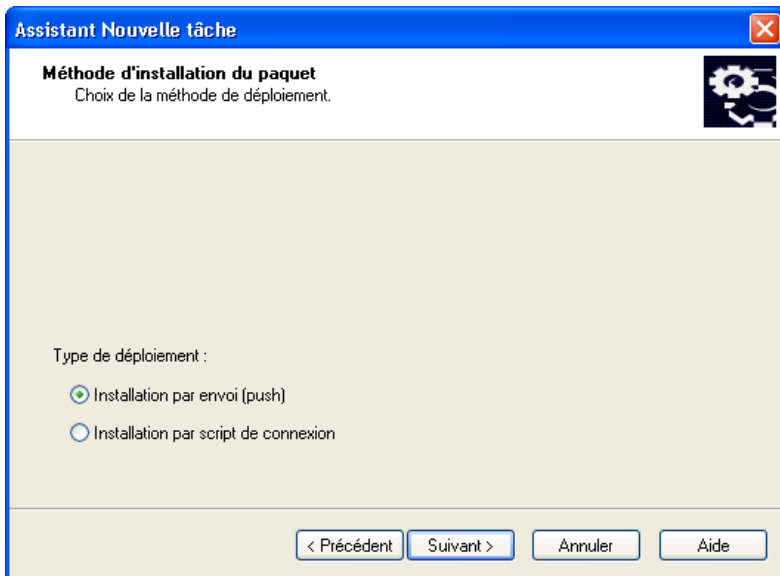


Illustration 31. Sélection de la méthode d'installation

7. Cette fenêtre de l'assistant (cf. ill. 32) vous permet de définir des paramètres d'installation complémentaires :

- Nécessité de réinstaller l'application si elle est déjà installée sur l'ordinateur.

Cochez la case **Ne pas installer sur des hôtes où ce produit est déjà installé** afin de ne pas procéder à une nouvelle installation (case cochée par défaut). Dans ce cas, la tâche ne sera pas lancée pour les ordinateurs où l'application est déjà installée localement ou suite à l'exécution antérieure d'une tâche d'installation programmée à distance.

Si la case est désélectionnée, la tâche d'installation à distance sera exécutée selon l'horaire défini jusqu'à ce que les tentatives d'installation aient été épuisées.

- Définir le mode de livraison des fichiers indispensables à l'installation de l'application sur les postes clients.

Pour ce faire, dans le groupe de champs **Télécharger le paquet d'installation** :

- Cochez la case **Télécharger le paquet à l'aide de dossiers partagés** afin de réaliser le transfert des fichiers indispensables à l'application sur les postes clients à l'aide des outils Windows via le dossier partagé (case cochée par défaut).
- Cochez la case **Télécharger le paquet avec l'agent réseau** pour que le transfert des fichiers sur les postes clients s'opère via l'agent de réseau installé sur chacun d'entre eux (case cochée par défaut).
- Définissez le nombre maximum de postes clients qui peuvent télécharger simultanément les informations du serveur d'administration dans le champ **Nombre maximum de téléchargements simultanés**.
- Définissez le nombre de tentatives d'installation au moment du lancement de la tâche programmée en saisissant la valeur souhaitée dans le champ **Nombre de tentatives**. Un nouvel essai sera tenté en cas d'erreur lors de l'exécution de l'essai précédent.

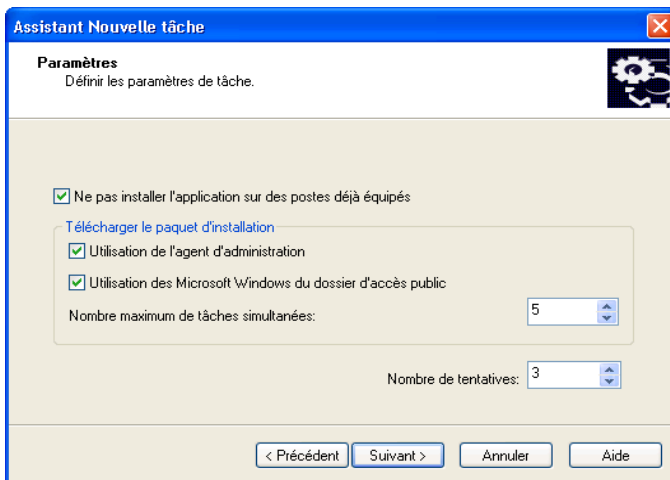


Illustration 32. Paramètres d'installation complémentaires

8. Cette étape (cf. ill. 33) vous propose d'installer également l'agent réseau.

Nous vous recommandons d'utiliser l'installation conjointe afin de réduire la charge du serveur d'administration. Pour ce faire, cochez la case **Installer avec l'agent réseau** et cochez la case en regard du paquet

d'installation requis. Le cas échéant, il est possible de créer un nouveau paquet d'installation à l'aide du bouton **Créer**.

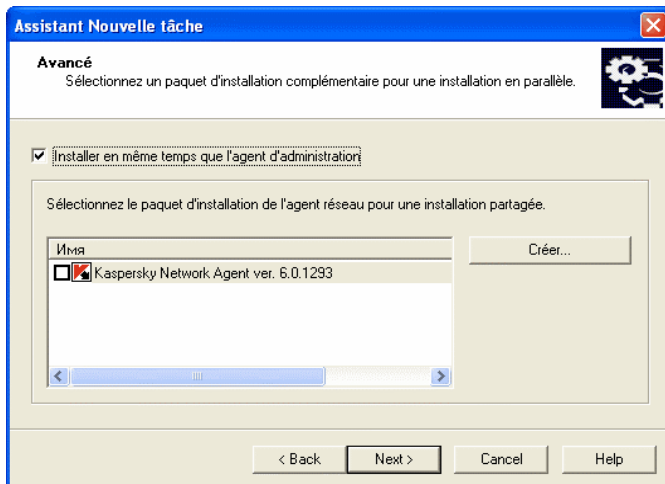


Illustration 33. Sélection de l'installation conjointe à l'agent réseau

9. Définissez le mode de sélection des ordinateurs pour lesquels la tâche est créée (cf. ill. 34) :
 - **Sur la base des données obtenues lors du sondage du réseau Windows.** Dans ce cas, la sélection des ordinateurs s'opère sur la base des données obtenues par le serveur d'administration lors du sondage du réseau Windows de l'entreprise.
 - **Sur la base de l'adresse IP des ordinateurs saisie manuellement.** Dans ce cas, les ordinateurs seront sélectionnés manuellement.

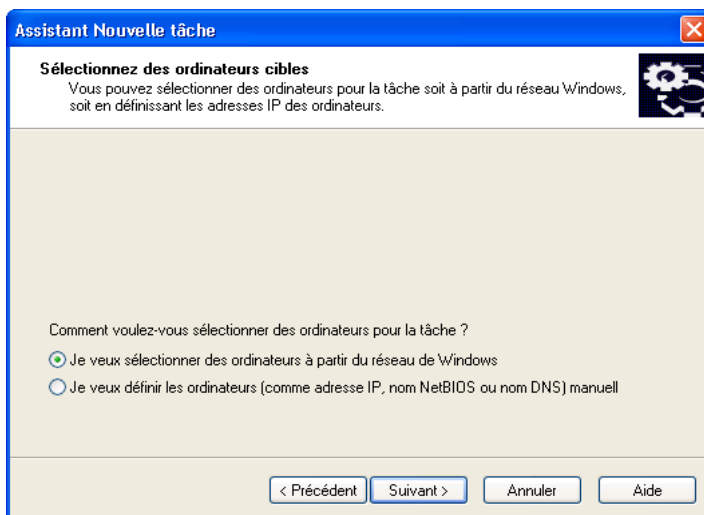


Illustration 34. Choix du mode de sélection des postes clients

Lorsque la sélection d'ordinateurs s'opère sur la base de données obtenues lors du sondage du réseau Windows, la liste est constituée dans la fenêtre de l'assistant (cf. ill. 35) de la même manière que lors de l'ajout de postes au réseau logique (pour de plus amples informations, consultez le manuel de l'utilisateur de Kaspersky Administration Kit). Vous pouvez choisir des postes clients du réseau logique (dossier **Groupes**) ou des postes qui n'en font pas encore partie (dossier **Réseau**).

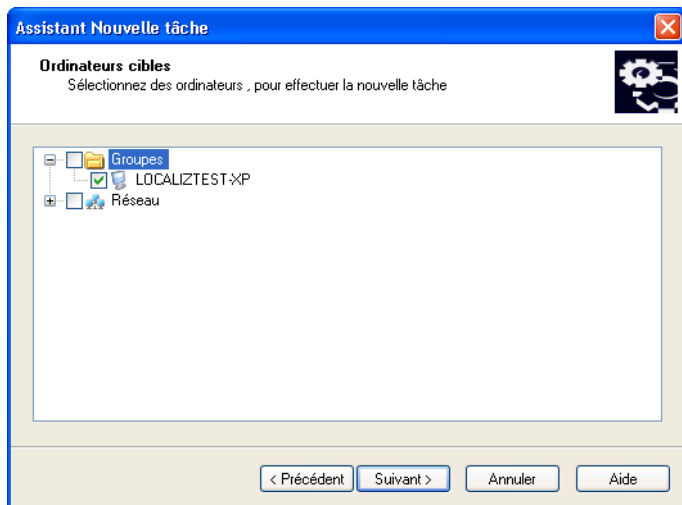


Illustration 35. Constitution de la liste d'ordinateurs sur la base des données du réseau Windows

Si la sélection s'opère manuellement, alors la constitution de la liste se fera en saisissant le nom NETBIOS ou DNS, les adresses IP (ou les plages d'adresse) des ordinateurs ou en important la liste dans un fichier *txt* où chaque nouvelle adresse doit figurer sur une nouvelle ligne (cf. ill. 36).

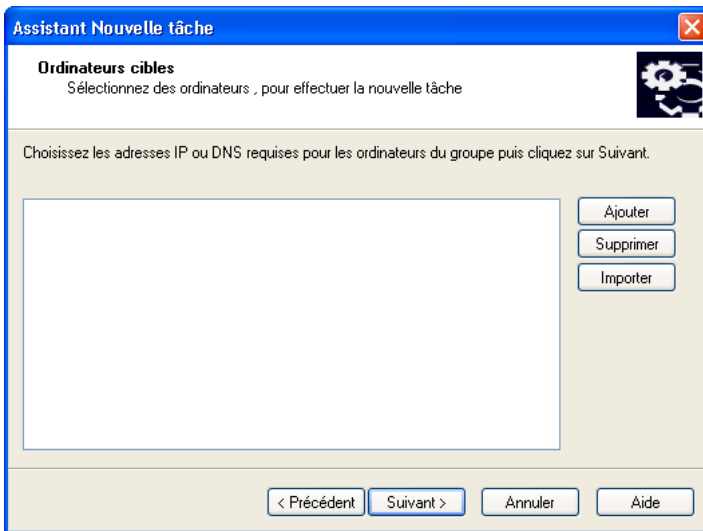


Illustration 36. Constitution d'une liste d'ordinateurs sur la base des adresses IP

10. Dans la fenêtre suivante de l'Assistant, définissez le compte utilisé pour démarrer la tâche d'installation à distance sur les ordinateurs (cf. ill. 37).

Le compte utilisateur doit avoir des droits d'administrateur sur tous les ordinateurs sur lesquels vous prévoyez d'exécuter la tâche de déploiement d'application.

Si vous installez des applications sur des ordinateurs qui appartiennent à différents domaines, des relations d'approbation doivent être activées entre les domaines respectifs du poste client et du serveur d'administration

Sélectionnez une des options suivantes :

- **Compte par défaut** – Exécute la tâche sous le compte par défaut si le serveur d'administration est lancé sous un compte d'utilisateur de domaine (cf. point 3.2, 18).
- **Compte spécifié** – Exécute la tâche sous le compte utilisateur spécifié, si le serveur d'administration est lancé sous le compte **Système local**, ou si le compte de service du serveur d'administration n'a pas de privilèges pour exécuter des tâches d'installation à distance.

Pour installer des applications Kaspersky sur les clients qui n'appartiennent pas à ce domaine, ouvrez une session en tant qu'utilisateur avec des privilèges d'administrateur, pour que ces clients puissent démarrer la tâche d'installation à distance.

Dans les zones ci-dessous, indiquez les informations sur l'utilisateur dont le compte satisfait les conditions requises.

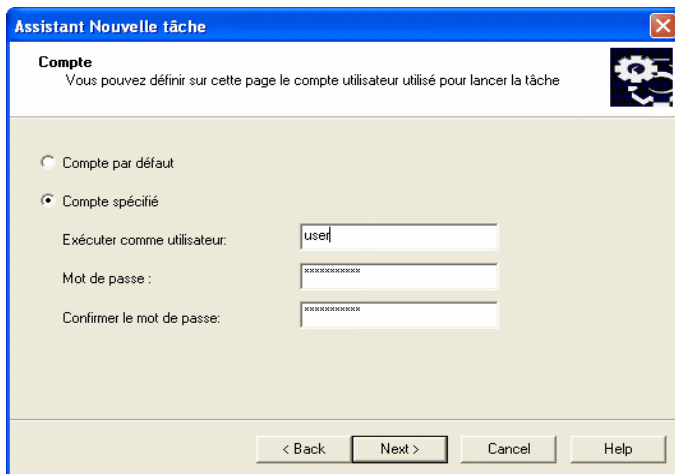


Illustration 37. Sélection du compte

11. Définition de la planification de la tâche (cf. ill. 38).

- Dans la liste **Planification à exécuter**, choisissez l'une des options suivantes :
 - **Manuellement**
 - **Toutes les N heures**
 - **Chaque jour**
 - **Chaque semaine**
 - **Chaque mois**
 - **Une fois** – Lance la tâche de déploiement d'application une fois seulement, indépendamment des résultats de la tâche.

- **Immédiatement** – Démarre la tâche immédiatement après avoir terminé l'Assistant.
- **À la suite d'une autre tâche** – Démarre la tâche d'installation à distance lorsque la tâche définie est terminée.
- Configurez les paramètres de programme dans les zones correspondant au mode de démarrage choisi (pour de plus amples informations, consultez le guide de Kaspersky Administration Kit).

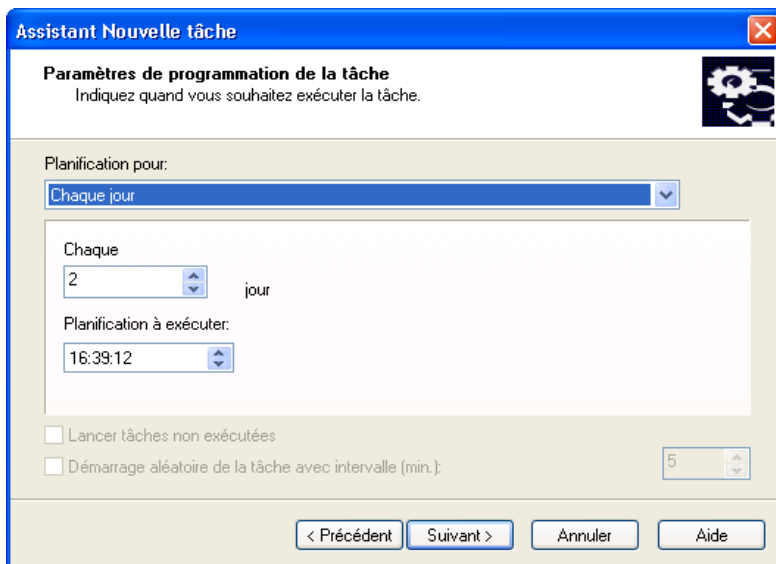


Illustration 38. Exécution quotidienne d'une tâche

Pour créer une tâche globale d'installation à distance selon la méthode d'installation par script de connexion :

1. Connectez-vous au serveur d'administration souhaité.
2. Sélectionnez le nœud **Tâches globales** dans l'arborescence de la console, affichez le menu contextuel et sélectionnez le point **Nouveau/Tâche** ou choisissez l'élément équivalent du menu **Action**. Cette action entraîne le lancement de l'Assistant de création de tâche. Suivez les instructions qui s'affichent.
3. Définissez le nom de la tâche.

4. Lors de la sélection de l'application et de la définition du type de tâche (cf. ill. 29), sélectionnez les valeurs **Kaspersky Administration Kit** et **Installation distante de l'application**.
5. Dans la fenêtre suivante (cf. ill. 30), indiquez le paquet d'installation à installer. L'opération est identique à celle de l'utilisation de l'installation par envoi (cf. ci-dessus).
6. Choisissez l'option **Utiliser un script de connexion pour l'installation** (cf. ill. 31).
7. Dans la fenêtre suivante de l'Assistant (cf. ill. 39), sélectionnez les comptes utilisateurs qu'il faut absolument modifier dans le script de connexion.

Au démarrage de la tâche d'installation, Kaspersky Administration Kit vérifie que l'utilisateur n'a pas défini de scénario de démarrage en plus de ceux sélectionnés. Le cas échéant, l'installation est interrompue. Dans ce cas, le rapport reprendra des informations sur l'erreur correspondante.

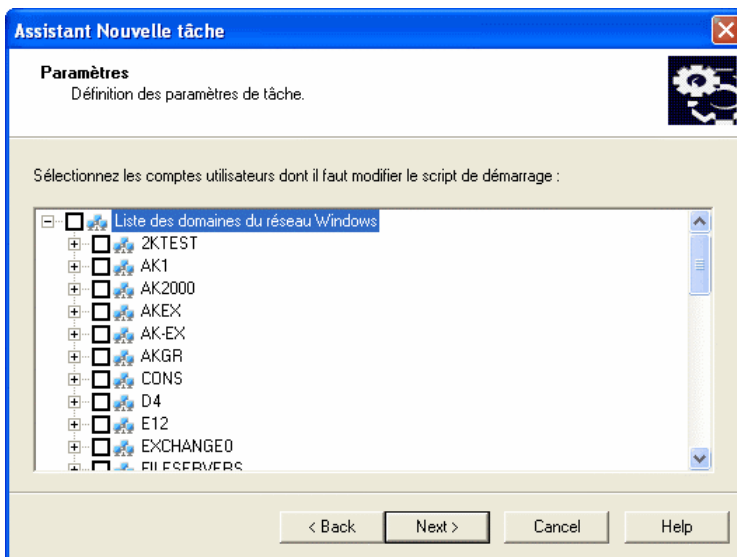


Illustration 39. Sélection des comptes utilisateur

8. A l'étape suivante (cf. ill. 37), tout comme lors de l'installation par envoi (cf. ci-dessus), indiquez le compte utilisateur qui servira pour l'exécution de l'installation à distance sur les postes clients.

9. Dans la fenêtre Programmation de la tâche (cf. ill. 38), programmez la tâche comme pour l'installation par envoi (cf. ci-dessus).

A la fin de la création de la tâche d'installation à distance, la nouvelle tâche sera reprise dans le nœud **Tâches globales** de l'arborescence de la console et apparaîtra dans le panneau des résultats. Le cas échéant, vous pourrez modifier les paramètres (pour de plus amples informations, consultez le point 4.1.8 à la page 67).

Pour ce faire :

déployez l'entrée **Installation distante** dans l'arborescence de console, sélectionnez le paquet d'installation requis dans le panneau de résultats et utilisez la commande **Installer** dans le menu contextuel ou dans le menu **Actions**. Ceci lance l'Assistant de tâche décrit ci-dessus. Cet Assistant omet la sélection du type de tâche et du groupe d'ordinateurs. Suivez les instructions de l'Assistant.

Il est possible également de lancer l'assistant de création d'une tâche de groupe d'installation à distance.

Pour ce faire :

Sélectionnez l'entrée correspondant au groupe souhaité dans l'arborescence de console, et cliquez sur **Installer** dans le menu contextuel ou dans le menu **Action**. L'assistant de tâche de déploiement d'applications démarre. Cet Assistant omet la sélection du type de tâche et du groupe d'ordinateurs. Suivez les instructions de l'Assistant.

4.1.8. Configuration de la tâche d'installation à distance

La tâche d'installation à distance est configurée de la même manière que les autres tâches (pour de plus amples informations, consultez le guide de Kaspersky Administration Kit). Par conséquent, nous ne décrivons parmi les paramètres présentés dans l'onglet **Paramètres**, que ceux qui sont spécifiques à chaque type de tâche.

En cas de modification d'une tâche qui réaliser une installation à distance par envoi (cf. ill. 40), vous pouvez :

- Choisir de réinstaller une application existante sur un client.
- Indiquer comment les fichiers d'installation seront transmis aux clients et définir le nombre maximum de connexions simultanées.

- Déterminer le nombre de tentatives de démarrage de cette tâche (si la tâche est planifiée).

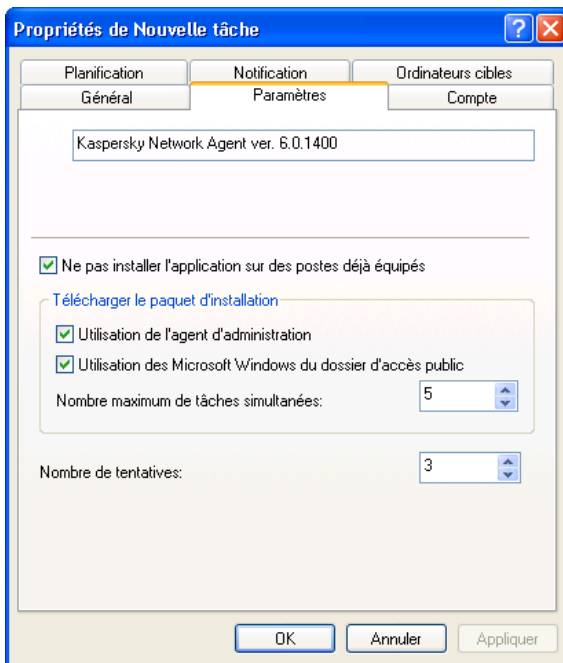


Illustration 40. Configuration d'une tâche d'installation à distance.
Installation par envoi

Si vous configurez une tâche d'installation par script de connexion, vous pouvez modifier dans l'onglet **Paramètres** la liste de comptes d'utilisateur auxquels les modifications seront applicables (cf. ill. 41). Utilisez les boutons **Ajouter** et **Supprimer** pour modifier la liste.

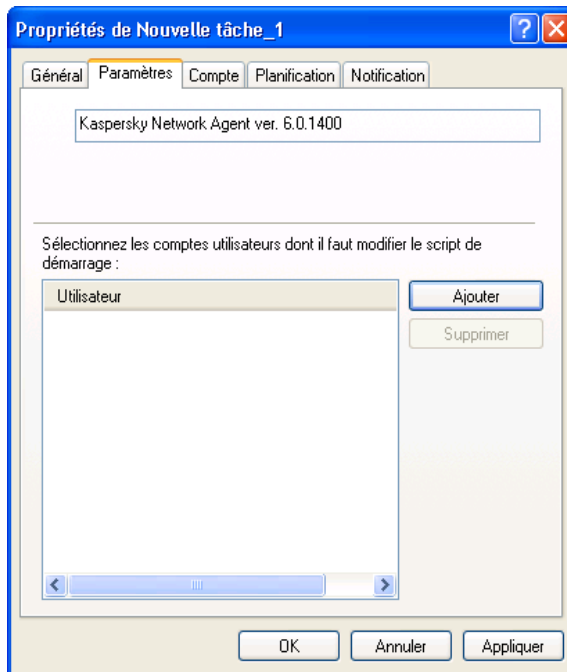


Illustration 41. Configuration de la tâche d'installation à distance à l'aide de scripts

4.1.9. Installation à distance d'une application sur les serveurs d'administration secondaires

Cette tâche permet d'installer et de mettre à jour des programmes sur les serveurs d'administration secondaires.

Pour créer une tâche de groupe visant à installer à distance une application sur les serveurs d'administration secondaires :

1. Connectez-vous au serveur d'administration.
2. Choisissez l'entrée **Tâches de groupe** dans l'arborescence de la console (si vous souhaitez créer une tâche pour tous les serveurs secondaires du groupe) ou **Tâches globales** (si vous souhaitez créer une tâche pour certains serveurs secondaires). Ouvrez le

menu contextuel et sélectionnez la commande **Nouveau / Tâche** ou utilisez le point équivalent du menu **Action**. L'Assistant pour la création d'une tâche s'affiche. Suivez les instructions.

3. Indiquez le nom de tâche.
4. Lors du choix de l'application et du type de tâche (cf. ill. 30), sélectionnez les entrées **Kaspersky Administration Kit** et **Installation à distance d'une application sur les serveurs d'administration secondaires**.
5. Ensuite, indiquez le paquet d'installation qui permettra d'exécuter la tâche définie (cf. ill. 31).
6. Dans la fenêtre suivante (cf. ill. 43), cochez si nécessaire la case **Ne pas installer une application déjà installée**. La version précise de l'application déterminera alors si l'installation sera ou non effectuée.

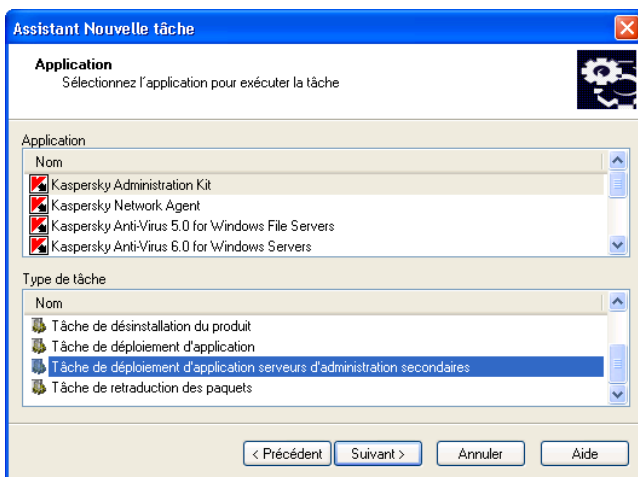


Illustration 42. Configuration de la tâche d'installation à distance d'une application sur les serveurs d'administration secondaires

7. Si vous créez une tâche de groupe, ignorez cette étape. Si vous créez une tâche globale, sélectionnez les serveurs d'administration secondaires dans la fenêtre **Serveurs d'administration secondaires** (cf. ill. 43).

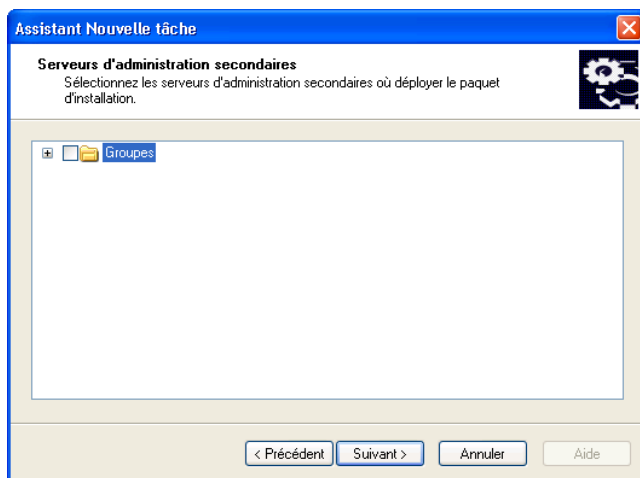


Illustration 43. Choix des serveurs d'administration secondaires

8. Planifiez la tâche.

Pendant la modification des paramètres des tâches de démarrage et d'arrêt de l'application, (cf. ill. 44), vous pouvez modifier les paramètres précédents.

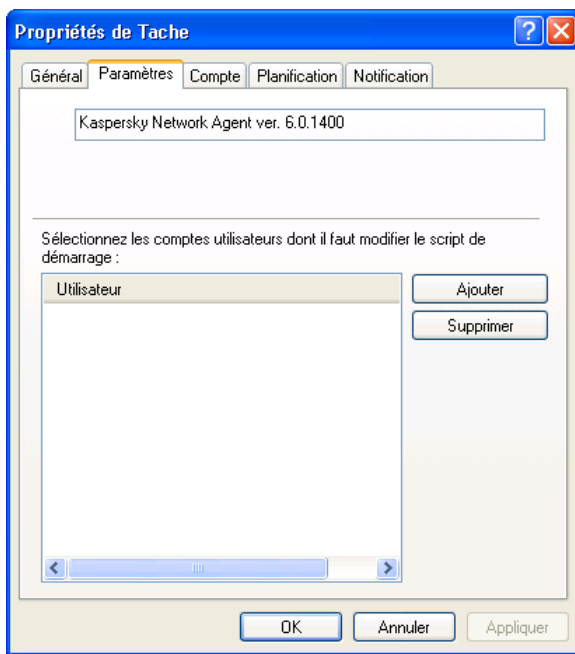


Illustration 44. Tâche d'installation d'une application sur les serveurs d'administration secondaires. Onglet **Paramètres**.

4.1.10. Désinstallation à distance d'une application

Pour procéder à la désinstallation à distance d'une application :

Créez une tâche comme pour l'installation à distance (cf. point 4.1.7, p. 55) et pour le type de tâche, sélectionnez **Désinstallation à distance** et dans la liste déroulante **Applications à désinstaller** de la fenêtre **Applications** (cf. ill. 45), sélectionnez l'application de Kaspersky Lab. Pour supprimer l'application d'un autre fabricant, cochez la case **Supprimer l'application d'un autre fabricant** et sélectionnez l'application à supprimer.

La liste déroulante reprend les applications découvertes sur les ordinateurs du réseau logique après l'installation de l'agent réseau

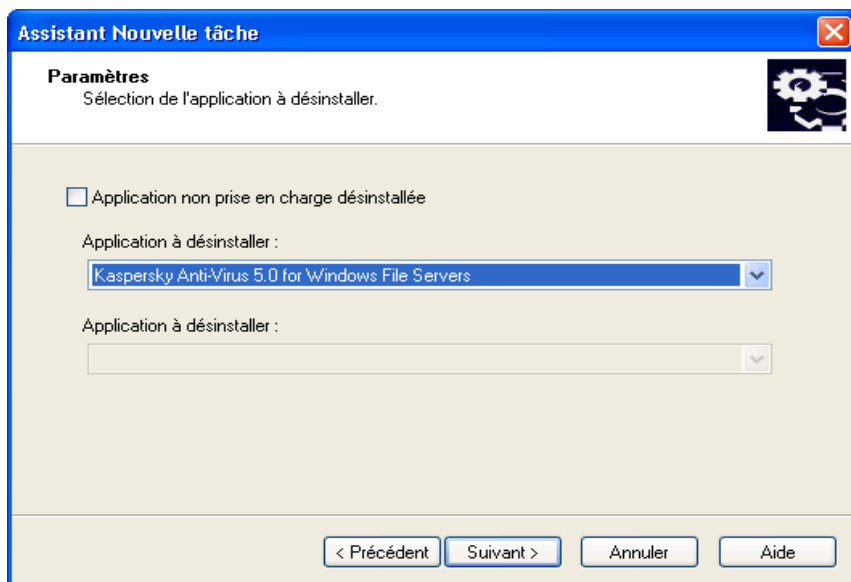


Illustration 45. Sélection d'une application à supprimer

La tâche ainsi créée sera exécutée selon l'horaire défini.

4.2. Assistant de déploiement d'application

Pour installer les applications de Kaspersky Lab, vous pouvez utiliser l'assistant de déploiement. Il vous permettra de procéder à l'installation par envoi, à l'aide de paquets d'installation ou directement au départ des fichiers d'installation.

L'Assistant contribue à :

- La création d'un paquet d'installation pour l'installation de l'application (s'il n'avait pas déjà été créé). Le paquet est placé dans le nœud **Installation distante**. Son nom correspond au nom et à la version de l'application et il peut être utilisé pour l'installation ultérieure de l'application.
- La création et le lancement de tâches globales ou de groupe d'installation à distance. La tâche créée est ajoutée au répertoire **Tâches globales** ou **Tâches de groupe** du groupe pour lequel elle a été créée. Elle pourra être lancée manuellement. Le nom de la tâche correspond au nom du

paquet d'installation de l'application : **Installation <nom du paquet d'installation sélectionné>**.

Pour installer l'application avec l'Assistant de déploiement d'application :

1. Connectez-vous au serveur d'administration.
2. Dans l'arborescence de console de la fenêtre principale de Kaspersky Administration Kit, sélectionnez le nœud correspondant au serveur d'administration souhaité et ouvrez le menu contextuel. Cliquez sur **Assistant de déploiement d'application** dans le menu contextuel ou dans le menu **Action** pour lancer l'Assistant. Suivez les instructions de l'Assistant.
3. Dans la boîte de dialogue qui s'affiche (cf. ill. 46), indiquez le paquet d'installation que vous allez utiliser. Si vous voulez installer une application à partir du fichier d'installation, ou si le paquet d'installation n'a pas encore été créé, créez un nouveau paquet d'installation. Pour ce faire, cliquez sur **Nouvelle...** pour lancer l'Assistant de création d'un paquet d'installation (cf. point 4.1.1, p. 40).

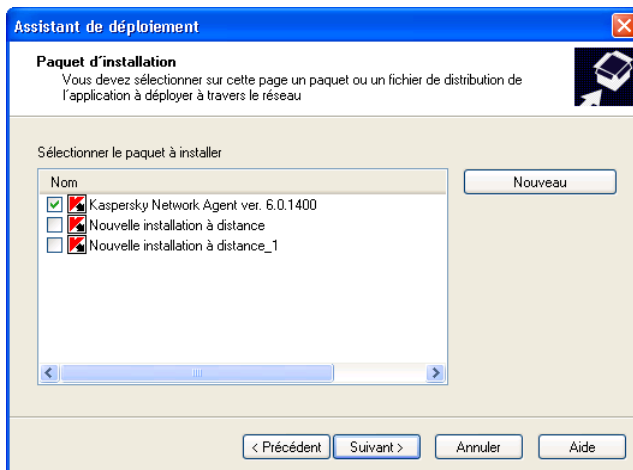


Illustration 46. Sélection du paquet d'installation

4. Dans la fenêtre suivante de l'assistant, indiquez au besoin le paquet d'installation de l'agent réseau pour une installation conjointe (pour de plus amples informations, consultez le point 4.1.7 à la page 55)

5. Spécifiez des ordinateurs sur lesquels vous souhaitez installer des applications Kaspersky Lab (cf. ill. 47) dans la fenêtre de l'Assistant. Sélectionnez l'une des options suivantes
- **Installer l'application sur les ordinateurs sélectionnés**, cette option permet de créer une tâche globale de déploiement d'application à la fin de l'Assistant.
 - **Installer l'application sur les ordinateurs du groupe administratif** – le résultat de l'Assistant est la création d'une tâche de groupe.

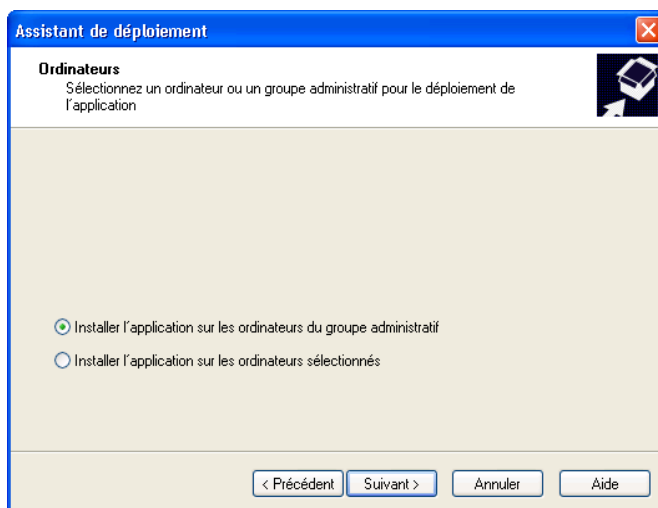


Illustration 47. Sélection du type de tâche

6. Ensuite, après la création d'une tâche de groupe, spécifiez le groupe dans lequel les applications vont être déployées (cf. ill. 48) ou sélectionnez des ordinateurs pour leur installation. Si l'application doit être installée sur les postes clients du réseau logique, sélectionnez le groupe **Groupes**.

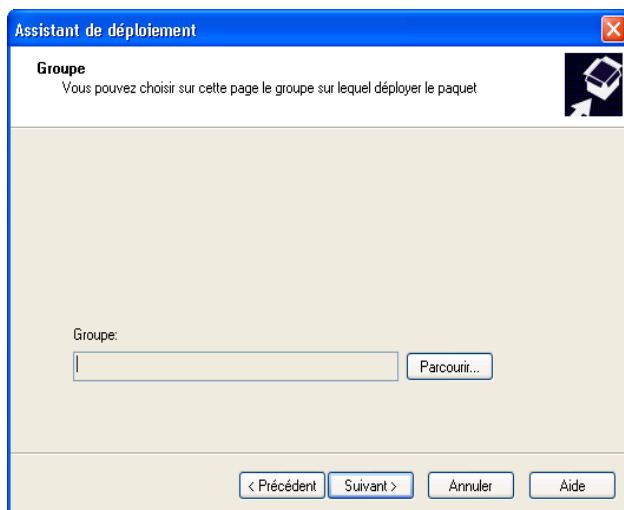


Illustration 48. Sélection du groupe

7. Vous devez ensuite spécifier le compte utilisé pour l'exécution de la tâche de déploiement sur les ordinateurs (pour de plus amples informations, consultez le point 4.1.7 à la page. 55).

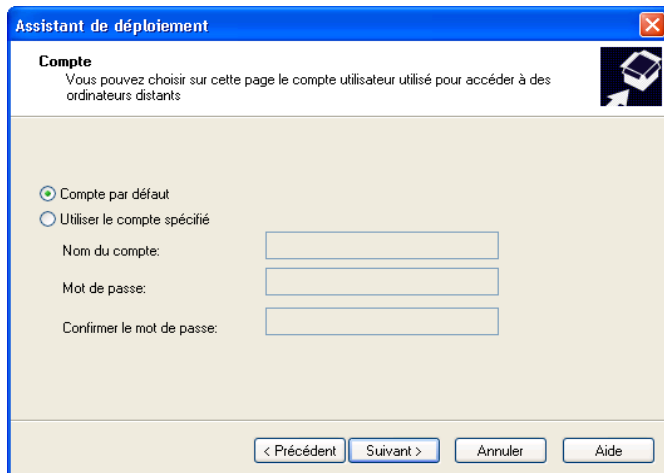


Illustration 49. Sélection du compte utilisateur

8. La fenêtre qui s'affiche ensuite illustre le processus de diffusion et d'exécution de la tâche d'installation sur les ordinateurs du groupe sélectionné (cf. ill. 50). Vous passez à la dernière fenêtre de l'Assistant sans attendre la fin du processus. Pour ce faire, cliquez sur **Suivant**. Pour afficher les détails d'exécution de la tâche sur des clients séparés, cliquez sur **Résultats**.

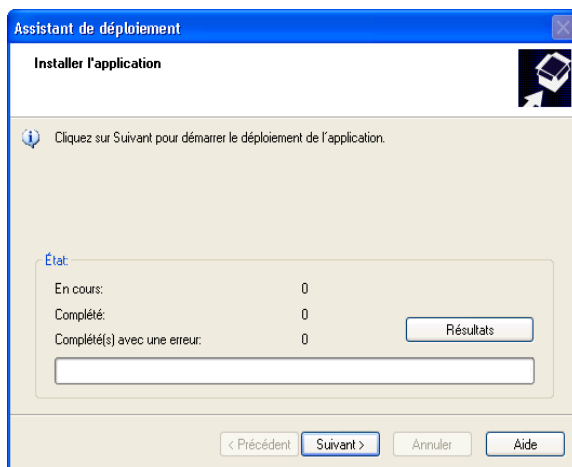


Illustration 50. Exécution d'une tâche de déploiement

4.3. Installation locale des applications

L'installation locale est effectuée séparément sur chaque ordinateur. Pour installer une application en local, vous devez posséder des privilèges d'administrateur sur l'ordinateur en local.

Plusieurs applications administrées à l'aide de Kaspersky Administration Kit peuvent être installées uniquement localement. Pour obtenir de plus amples informations, consultez les guides des applications correspondantes.

Vous pouvez effectuer une installation local sur le poste client via la Console d'administration en utilisant une connexion au bureau à distance.

La méthodologie d'installation en local des applications Kaspersky Lab pourrait être la suivante :

- Installez l'agent réseau et établissez la connexion entre le client et le serveur d'administration (cf. point 4.3.1, p. 78).
- Installez les applications requises sur les ordinateurs présents dans le système de protection antivirus, en suivant les instructions fournies par la documentation de ces applications.
- Installez le plug-in d'administration correspondant à chaque application installée sur le poste administrateur (cf. point 4.3.2, p. 83).

Kaspersky Administration Kit prend en charge l'installation locale des applications en mode silencieux, à partir des fichiers créés lors de la génération du paquet d'installation (cf. point 4.3.3, p. 84).

4.3.1. Installation locale de l'agent réseau

Pour installer l'agent réseau en local :

1. Exécutez le fichier **setup.exe** (ou **setup.msi**) dans le dossier **NetAgent** du CD d'installation de Kaspersky Administration Kit. L'Assistant d'installation vous invite à configurer les paramètres d'installation. Suivez les instructions de l'Assistant.
2. Les premières étapes de l'installation couvrent la récupération et la copie de fichiers sur votre disque dur, l'acceptation du contrat de licence, et la saisie des informations utilisateur.
3. Ensuite, indiquez le dossier de destination de Network Agent. L'emplacement par défaut est **Program Files\Kaspersky Lab\NetworkAgent**. Si ce dossier n'existe pas, il sera créé automatiquement. Cliquez sur **Parcourir** pour sélectionner un autre emplacement.
4. Dans la fenêtre suivante de l'Assistant (cf. ill. 51), indiquez les paramètres suivants, afin que Network Agent puisse se connecter au serveur d'administration :
 - Le champ **Adresse du serveur** contient l'adresse de l'ordinateur sur lequel est ou va être exploité le serveur d'administration. Vous pouvez utiliser une adresse IP ou le nom de l'ordinateur sur le réseau Windows. Vous pouvez également choisir l'ordinateur à l'aide du bouton **Parcourir**.
 - Si nécessaire, ouvrir le port UDP 137, utilisé pour la réception de l'adresse IP du serveur d'administration, dans le dispositif

anti-piratage de Kaspersky Anti-Virus 6.0. Pour ce faire, cochez la case **Permettre service du nom NetBIOS en Anti-hacker**.

- Le champ **Port du serveur** donne le numéro de port utilisé par Network Agent pour se connecter au serveur d'administration. Le port par défaut est **14000**. Si ce port est déjà en service, vous pouvez en changer. N'utilisez que des multiples de dix.
- Le champ **Port SSL du serveur** donne le numéro de port utilisé pour une connexion SSL au serveur d'administration. Le port par défaut est **13000**. Si ce port est déjà en service, vous pouvez en changer. N'utilisez que des multiples de dix dans ce champ. Pour activer la connexion SSL, cochez la case **Utiliser SSL pour se connecter au serveur**.

Assistant d'installation - Kaspersky Network Agent

Serveur d'administration

Sélectionnez un Administration Server

Sélectionnez l'ordinateur où Kaspersky Administration Server est installé.

Adresse du serveur :

Définir le port de Administration Server. La valeur doit se trouver dans l'intervalle 1-65535.

Port du serveur :

Définir le port SSL de Administration Server. La valeur doit se trouver dans l'intervalle 1-65535.

Port SSL du serveur :

☒ Utiliser SSL pour se connecter au serveur

< Précédent Suivant > Annuler

Illustration 51. Configuration des paramètres de connexion au serveur d'administration

5. Si la connexion de l'agent réseau au serveur d'administration s'opère via un serveur proxy, configurez les paramètres de connexion dans la fenêtre (cf. ill. 52) :
- Cochez la case **Utiliser le serveur proxy pour la connexion au serveur d'administration** et saisissez l'adresse et le numéro du port de connexion. Seule la notation décimale est autorisée (par exemple : **Adresse du serveur proxy** : proxy.test.ru, **Port** : 8080).

- Si l'accès au serveur proxy requiert un mot de passe, remplissez les champs **Nom d'utilisateur** et **Mot de passe**.

Si vous n'utilisez pas de serveur proxy, passez cette étape en cliquant sur **Suivant**.

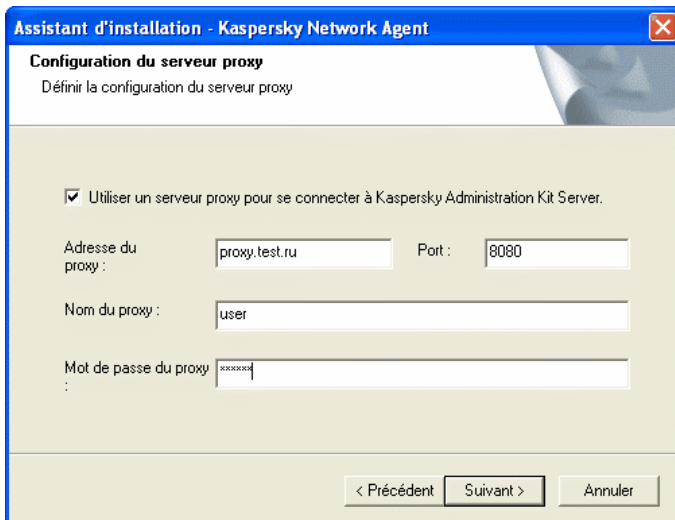


Illustration 52. Configuration de la connexion au serveur proxy

6. Spécifiez le dossier du groupe **Non attribué** où ce client sera ajouté par le serveur d'administration. Indiquez les options suivantes (cf. ill. 53):
 - **Nom de groupe par défaut** – Le client sera ajouté à un dossier qui correspond à son emplacement courant dans le réseau Windows – domaine ou groupe d'utilisateur (option active par défaut).
 - **Définir le nom de groupe** – Le client sera ajouté au dossier indiqué. Écrivez le nom du dossier dans la zone inférieure. Si le groupe **Non attribué** ne possède aucun dossier avec ce nom, il sera créé (vous pouvez également indiquer le nom du dossier existant dans le groupe **Non attribué**).

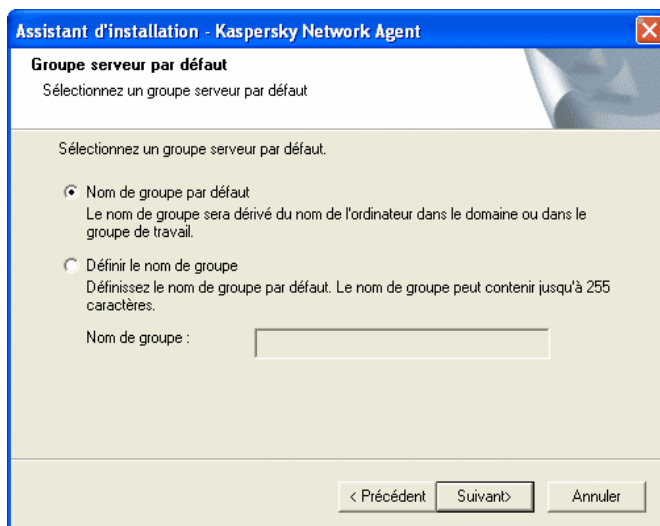


Illustration 53. Définition du groupe de stockage des ordinateurs dans le dossier **Non attribué**

7. À l'étape suivante (cf. ill. 54), indiquez comment le certificat du serveur d'administration sera récupéré. Sélectionnez l'une des options suivantes :
- **Fichier de certification par défaut** – le certificat du serveur d'administration sera envoyé lors de la première connexion de Network Agent au serveur d'administration (valeur par défaut).
 - **Sélectionnez un fichier de certification** – Le serveur d'administration sera authentifié en utilisant un certificat choisi par l'administrateur. Cliquez sur Parcourir pour retrouver le fichier nécessaire.

Le fichier possède une extension **.cer** et se trouve placé dans le dossier **Cert** du répertoire de Kaspersky Administration Kit sur le serveur d'administration. Vous pouvez copier le fichier de certification dans un dossier partagé ou une disquette. Cette copie peut être utilisée pendant l'installation de l'agent réseau.

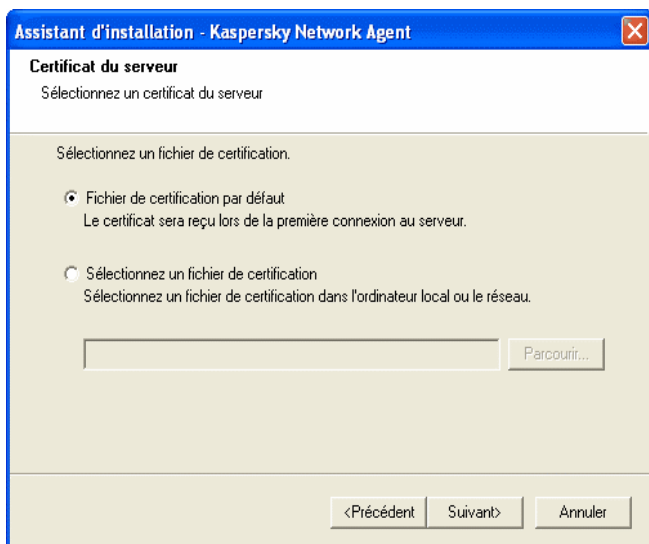


Illustration 54. Choix d'une méthode de réception du certificat du serveur d'administration

8. Dans la dernière boîte de dialogue de l'Assistant (cf. ill. 55), cochez la case **Exécuter l'agent réseau** pour lancer Network Agent juste après la fin de l'installation. Si vous voulez lancer Network Agent plus tard, annulez la sélection de cette case.

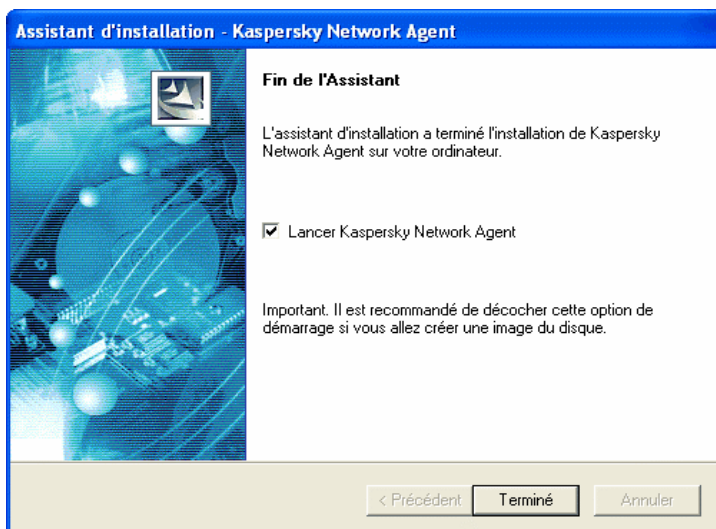


Illustration 55. Configuration du lancement de l'agent réseau

À la fin de l'installation, Network Agent sera installé sur votre ordinateur avec les paramètres suivants .

Vous pouvez afficher les propriétés du service **Kaspersky Network Agent**, le lancer et l'arrêter, et surveiller son exécution à partir de l'outil **Services**, qui est l'outil standard d'administration de Windows.

Le plug-in permettant la collaboration avec Cisco Network Admission Control (NAC) est systématiquement installé avec l'agent d'administration. Il n'est toutefois activé que lorsque l'application Cisco Trust Agent est installée sur l'ordinateur.

4.3.2. Installation locale du plug-in d'administration des applications

Pour installer le plug in d'administration de l'application,

Exécutez le fichier **klcfginst.exe**, dans le CD d'installation de l'application, sur l'ordinateur de l'ordinateur disposant de la console d'administration. Ce fichier est inclus avec toutes les applications pouvant

être contrôlées par Kaspersky Administration Kit. L'installation est effectuée à l'aide d'un assistant et ne nécessite aucune configuration.

Le fichier d'installation de Agent Réseau (**klcfginst.exe**) se trouve dans le dossier **NetAgent** du paquet d'installation de Kaspersky Administration Kit.

4.3.3. Installation d'applications en mode silencieux

Pour installer une application en mode silencieux :

1. Créez le paquet d'installation nécessaire (voir section 4.1.1 à la page 40) si vous ne l'avez pas fait pour cette application.

Des paquets d'installation seront entreposés sur le serveur d'administration dans le dossier **Packages**, dans un dossier partagé spécifié pendant l'installation du serveur d'administration. Chaque paquet d'installation disposera de son propre répertoire.

2. Le cas échéant, modifier les paramètres du paquet d'installation (pour plus de détails, voir la section 4.1.2 à la page 41).
3. Choisissez le type d'installation :

Copiez le dossier entier correspondant au paquet d'installation souhaité à partir du serveur d'administration vers le poste client. Sur le poste client, ouvrez le dossier copié et lancez le fichier exécutable (fichier avec l'extension **.exe**) avec le commutateur **/s**.

ou

À partir du poste client, ouvrez le dossier partagé sur le serveur d'administration correspondant au paquet d'installation souhaité. Lancez ensuite le fichier exécutable avec le commutateur **/s**.

Si Kaspersky Administration Kit est installé en mode non-interactif, vous pouvez utiliser le fichier de paramètres. Ce fichier contient tous les paramètres d'installation de l'application, ce qui permet d'effectuer une installation multiple en ne spécifiant qu'une fois les paramètres.

Pour créer un fichier de paramètres Kaspersky Administration Kit :

1. En ligne de commande, positionnez-vous dans le répertoire d'installation de Kaspersky Administration Kit et lancez le fichier exécutable avec les

commutateurs **/r /f1"<chemin du fichier>\setup.iss"**³ (par exemple, **setup.exe /r /f1"C:\setip.iss"**).

L'assistant d'installation est alors démarré.

2. Complétez les paramètres d'installation en suivant les instructions de l'assistant. Il est par exemple possible de sélectionner l'installation du serveur d'administration ou uniquement de la console (cf. ill. 3.2 à la page 19).

Une fois l'installation terminée, la version sélectionnée de Kaspersky Administration Kit sera installée et le fichier de paramètres sera créé dans le répertoire indiqué. Copiez ensuite le fichier de paramètres sur le serveur d'administration, dans le dossier du paquet d'installation concerné. Lors d'installations ultérieures de Kaspersky Administration Kit en mode non-interactif, les paramètres du fichier seront automatiquement utilisés.

Le fichier de paramètres permet la mise à jour de Kaspersky Administration Kit en mode non-interactif. De cette manière, il n'installera que les mises à jour de la version sur base de laquelle il a été créé.}

³ Spécifiez le chemin complet du fichier de paramètres.

ANNEXE A. GLOSSAIRE

Cette documentation utilise certains termes spécialement liés à la protection antivirus. Le glossaire présente une liste des définitions de ces termes. Les entrées de glossaire sont classées par ordre alphabétique afin d'en faciliter la consultation.

A

Administrateur de réseau logique – Utilisateur qui installe, configure et met à jour Kaspersky Administration Kit, et qui contrôle à distance les applications Kaspersky Lab installé sur les ordinateurs du réseau logique.

Agent de mise à jour – Ordinateurs qui font office d'intermédiaires pour la diffusion des mises à jour et des paquets d'installation dans les limites du groupe.

Analyse complète à la demande – Mode défini par l'administrateur, qui analyse tous les fichiers de l'ordinateur à la recherche de virus et qui désinfecte ou supprime les objets infectés après leur détection.

Analyse de fichier par format – Mode d'analyse selon lequel le programme analyse le contenu d'un fichier, à savoir, l'identificateur de format de l'en-tête de fichier.

Analyse de fichiers par extension – En mode d'analyse, le programme tient compte de l'extension du fichier analysé.

Applications d'autres fabricants: application antivirus d'un autre éditeur ou application de Kaspersky Lab qui n'est pas administrée par Kaspersky Administration Kit.

B

Base antivirus – Base de données créée par les spécialistes de Kaspersky Lab, contenant des définitions détaillées de tous les virus existants, avec des procédés de détection et de désinfection. Les applications antivirus utilisent cette base de données afin de détecter et de désinfecter les virus avec succès. La base antivirus disponible sur les sites Web de Kaspersky Lab est régulièrement mise à jour au fur et à mesure de l'apparition de nouvelles menaces de virus. Les utilisateurs enregistrés de Kaspersky Lab ont accès aux mises à jour des bases de données. Pour conserver votre ordinateur constamment protégé contre des virus, nous recommandons de télécharger régulièrement les mises à jour.

Bases de messagerie – Bases de données contenant les messages de courrier entreposés sur votre ordinateur. Chaque message entrant/sortant est enregistré dans la base de données après sa réception/son envoi. Ces bases de données sont analysées en mode d'analyse à la demande.

Blocage d'objet – Évite que des applications externes puissent accéder à un objet. L'objet bloqué ne peut pas être lu, exécuté, modifié ni supprimé.

C

Certificat du serveur d'administration – Certificat permettant d'authentifier la connexion de la console d'administration au serveur d'administration, et les transferts de données entre le serveur et les clients. Le certificat du serveur d'administration est créé pendant l'installation du serveur d'administration. Il est placé dans le sous-dossier **Cert** du dossier d'installation.

Clé de licence – Fichier avec extension **.key** utilisé comme "clef" personnelle. Ce fichier est nécessaire pour un fonctionnement correct des applications Kaspersky Lab. Vous trouverez la clé de licence dans le kit de distribution si vous avez acheté l'application chez un distributeur Kaspersky Lab. Si vous avez acheté l'application en ligne, la clé de licence vous est envoyée à travers un courrier électronique. Sans clé de licence, Kaspersky Anti-Virus NE FONCTIONNE PAS.

Client du serveur d'administration (ou **poste client**) – un ordinateur, un serveur ou une station de travail sur lequel sont exploités le composant Network Agent et les applications Kaspersky Lab.

Console d'administration – Composant de Kaspersky Administration Kit qui fournit l'interface des services administratifs de Administration Server et de Network Agent.

D

Désinfection – Un procédé de traitement des objets infectés. La désinfection implique la restauration partielle ou totale des données, ou la conclusion que ces fichiers ne peuvent pas être désinfectés. Les objets sont désinfectés à l'aide de la base antivirus. Si la désinfection est la première action appliquée après la détection d'un objet suspect, par exemple, alors le programme effectue une sauvegarde du fichier. Si des données sont perdues pendant la désinfection, la sauvegarde permet de récupérer l'objet.

Disques virtuels (disques RAM) – Partie de RAM utilisée pour simuler un disque physique normal dans un ordinateur individuel.

E

Entrepôt de sauvegarde – Dossier contenant les copies de sauvegarde des données du serveur d'administration, créées par l'outil de sauvegarde.

État de la protection antivirus – Situation actuelle de la protection antivirus qui décrit le niveau de sécurité de votre ordinateur.

Exclusions – Configuration utilisateur permettant d'exclure certains objets des analyses. Vous pouvez adapter les règles d'exclusion à la *protection en temps réel* et à l'*analyse à la demande*. Vous pouvez ainsi

désactiver l'analyse des archives au cours d'une analyse complète, ou exclure des fichiers à l'aide de masques.

G

Gestion centralisée d'une application – Gestion d'une application à l'aide de Kaspersky Administration Kit.

Gestion locale – Gestion d'une application par l'intermédiaire d'une interface locale.

Groupe d'administration – Ordinateurs groupés selon des critères fonctionnels et applications de Kaspersky Lab installées. Le regroupement simplifie considérablement les procédures de gestion et permet à l'administrateur de gérer tous les ordinateurs sous la forme d'éléments simples. Un groupe peut inclure d'autres groupes. Des stratégies de groupe et des tâches de groupe peuvent être créées pour chaque application installée sur un membre du groupe.

I

IChecker – Technologie qui permet d'exclure des analyses suivantes les objets qui n'ont pas été modifiés depuis l'analyse précédente. La technologie IChecker repose sur la mise en place d'une base contenant les sommes de contrôle des objets.

Installation distante – Installation des applications Kaspersky Lab à l'aide des fonctions offertes par Kaspersky Administration Kit.

Installation par envoi – Méthode d'installation à distance (en anglais: Push) permettant d'installer le logiciel Kaspersky Lab sur des ordinateurs spécifiques de votre réseau logique. Pour réussir l'installation par envoi, le serveur d'administration doit disposer des privilèges nécessaires pour exécuter les applications sur les clients distants. Cette méthode est recommandée pour des ordinateurs sous MS Windows NT/2000/2003/XP, qui prennent en charge cette caractéristique, ou sur des ordinateurs sous MS Windows 98/Me, sur lesquels Network Agent est installé.

Installation par script – Méthode d'installation qui fait dépendre la tâche d'installation distante d'un ou de plusieurs comptes utilisateur spécifiques. Quand l'utilisateur spécifique ouvre une session sur le domaine, l'installation de l'application s'effectue sur le poste client utilisé. Cette méthode est recommandée pour des ordinateurs exploités sous MS Windows 95/98/Me

IStreams – Technologie qui permet d'exclure les fichiers stockés sur des disques au format NTFS, s'ils n'ont pas été modifiés depuis l'analyse précédente. La technologie IStreams est mise en œuvre grâce en conservant les sommes de contrôle des fichiers dans les flux NTFS supplémentaires.

K

Kaspersky Administration Kit – Application spécialisée dans l'exécution centralisée des tâches administratives principales. Il offre un contrôle complet sur la stratégie antivirus de l'entreprise utilisatrice d'applications Kaspersky Lab.

M

Mise à jour – Fonction de Kaspersky Anti-Virus qui met à jour des fichiers, ou en ajoute de nouveaux (base antivirus ou modules de programme), récupérés à partir des serveurs de mise à jour de Kaspersky Lab.

Mises à jour disponibles – Service Packs contenant des mises à jour urgentes, entreposées pendant un certain temps, ainsi que les dernières modifications dans l'architecture de l'application.

N

Network Agent (Network Agent) – Composant de Kaspersky Administration Kit qui se charge de la communication entre le serveur d'administration et les applications Kaspersky Lab installés sur les postes réseau spécifiques (stations de travail ou serveurs). Ce composant est commun à toutes les applications Windows comprises dans Kaspersky Lab Business Optimal et Corporate Suite. Il existe des versions de l'agent réseau spécifiques aux applications Kaspersky Lab tournant sur Novell ou Unix.

Niveau de gravité – Paramètre distinctif d'un événement enregistré au cours de l'exécution de Kaspersky Anti-Virus. Il y a quatre degrés de gravité :

- **Critique**
- **Erreur**
- **Avertissement**
- **Info**

Des événements de même type peuvent avoir différents degrés de gravité, en fonction du moment spécifique.

Niveau recommandé – Niveau de protection antivirus utilisant les paramètres recommandés par les experts de Kaspersky Lab, qui assure une protection optimale de votre ordinateur. Ce niveau est celui par défaut.

O

Objet infecté – Objet contenant un virus. Nous recommandons de cesser de travailler avec ces objets qui peuvent infecter votre ordinateur.

Objet suspect – Objet contenant une mutation de code d'un virus déjà connu, ou un code ressemblant à un virus mais encore inconnu des spécialistes de Kaspersky Lab.

Objets de démarrage – Un ensemble de programmes nécessaires pour le lancement et le bon fonctionnement du système d'exploitation, et du reste des logiciels installés dans l'ordinateur. Votre système d'exploitation lance ces objets à chaque démarrage. Certains virus tentent d'infecter ces objets et causent la défaillance du système au démarrage.

OLE (objet) – Objet lié ou incorporé dans d'autres fichiers utilisant la technologie OLE.

Opérateur de réseau logique – Utilisateur chargé de surveiller le système de protection antivirus contrôlé par Kaspersky Administration Kit.

P

Paquet d'installation – Un paquet de fichiers utilisé pour installer des applications Kaspersky Lab sur postes distants d'un réseau logique. Les paquets d'installation s'appuient sur un fichier **.kpd** spécial inclus dans le kit de distribution de l'application, avec les paramètres minimums assurant le fonctionnement de base de l'application après son installation. Ces paramètres correspondent aux paramètres par défaut des applications.

Paramètres d'application – Paramètres d'application communs à tous les types de tâches exécutées par cette application.

Paramètres de tâche – Paramètres d'application spécifiques pour chaque type de tâche.

Période de licence – Période pendant laquelle vous pouvez profiter de toutes les fonctions de Kaspersky Anti-Virus. En règle générale, la période de licence est d'un an, à compter de la date d'achat de la clé. Après l'expiration de la licence, l'application continuera de fonctionner mais il ne sera pas possible de mettre à jour la *base antivirus*.

Plug-in de console (gestion) – Composant spécial d'interface permettant de contrôler une application à distance à l'aide de la console d'administration. Les plug-ins sont spécifiques à chaque application et sont inclus dans toutes les applications Kaspersky Lab pouvant être contrôlées par Kaspersky Administration Kit.

Poste administrateur – Ordinateur sur lequel la console d'administration de Kaspersky Administration Kit est installée. Avec cette console, l'administrateur peut établir et contrôler un système de protection antivirus utilisant des applications Kaspersky Lab.

Protection en temps réel – Mode d'analyse dans lequel une application antivirus reste résidente en mémoire. Dans le mode de protection en temps réel, l'application analyse tous les objets ouverts en lecture, en écriture ou en exécution. Avant de permettre l'accès à un objet, Kaspersky Anti-Virus l'analyse et, s'il détecte un virus, bloque l'accès à l'objet, puis le désinfecte ou le supprime (selon la configuration utilisateur).

Protection Maximum – Niveau de protection qui garantit une protection complète mais pénalise légèrement le rendement.

Q

Quarantaine – Entrepôt spécial qui isole les objets infectés et suspects.

Quarantaine – Méthode de traitement d'un objet *suspect*. L'accès à l'objet est bloqué et le fichier est déplacé vers la quarantaine en vue d'un traitement postérieur.

R

Restauration – Restauration des données du serveur d'administration à l'aide d'un outil de sauvegarde. L'information de restauration est disponible dans l'entrepôt de sauvegarde. L'outil vous permet de restaurer :

- Base de données du serveur d'administration qui entrepose les stratégies, les tâches, les paramètres d'application, et les événements enregistrés sur le serveur d'administration;
- Informations sur les configurations des réseaux logiques et des clients ;
- Fichiers pour l'installation à distance des applications (contenu des dossiers Packages, Uninstall, Updates);
- Certificat du serveur d'administration

S

Sauvegarde (dossier de) – Répertoire contenant des copies de sauvegarde des objets effacés et désinfectés.

Sauvegarder – Créer une copie de sauvegarde d'un fichier dans un dossier de sauvegarde avant traitement (désinfection ou suppression). Par la suite, ce fichier peut être restauré à partir de sa sauvegarde, par exemple, pour son analyse postérieure à partir d'une base antivirus mise à jour.

Serveur d'administration – Composant de Kaspersky Administration Kit qui stocke de manière centralisée des informations sur les applications Kaspersky Lab installées sur les clients, et qui contrôle ces applications.

Serveurs de mise à jour de Kaspersky Lab – Liste de sites HTTP et FTP de Kaspersky Lab, d'où vous pouvez obtenir les mises à jour pour votre ordinateur.

Seuil d'activité virale – Nombre de virus détectés dans un intervalle de temps déterminé. Si ce nombre est dépassé, la situation est identifiée comme une **Attaque virale**. Ce paramètre est important dans l'identification des épidémies, car il détermine le temps de réaction administrative face à de nouvelles menaces, et l'application des mesures préventives destinées à protéger le réseau.

Stratégie – voir **Stratégie de groupe**

Stratégie de groupe – Ensemble des paramètres d'application d'un groupe administratif contrôlé par le Kaspersky Administration Kit. Les stratégies de groupe peuvent être différentes pour chaque groupe. Les stratégies de groupe sont spécifiques pour différentes applications. La stratégie détermine la configuration de tous les paramètres des applications.

Suppression d'un objet – Méthode de traitement d'un objet. La suppression d'un objet signifie l'enlever physiquement d'un ordinateur. Cette méthode est recommandée pour traiter les objets infectés. Si la suppression est la première action appliquée sur un objet, il est nécessaire d'en créer une copie de sauvegarde avant de le supprimer. Vous pouvez utiliser la sauvegarde pour restaurer l'objet original.

T

Tâche – Action nommée, qui est exécutée par une application de Kaspersky Lab.

Tâche de groupe – Tâche définie et utilisée pour tous les clients d'un groupe.

Tâche globale – Tâche définie et utilisée pour un certain nombre de clients de différents groupes administratifs.

Tâche locale – Tâche créée et utilisée sur un simple client.

V

Virus inconnu – Nouveau virus non répertorié dans la *base antivirus*. En règle générale, Kaspersky Antivirus détecte les virus inconnus grâce à un *analyseur de code heuristique*, et identifie les objets contenant ces virus comme *suspects*.

Vitesse maximum – Niveau de protection qui assure une vitesse maximum mais un degré moindre de sécurité.

ANNEXE B. KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

B.1. Autres produits antivirus

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la « météo » des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d'informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S'abonner et se désabonner aux canaux d'information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d'informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l'information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky® OnLine Scanner

Il s'agit d'un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l'ordinateur. Kaspersky OnLine Scanner est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s'agit d'un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l'ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro est exécuté directement dans le navigateur. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs questions sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html;

Kaspersky® Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers.** Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.
- **Observer les processus dans la mémoire vive.** Kaspersky Anti-Virus 7.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus actifs.
- **Surveiller les modifications de la base de registres système** grâce au contrôle de l'état de la base de registres.

- **Le contrôle des processus cachés** permet de lutter contre les outils de dissimulation d'activité qui cachent le code malveillant dans le système d'exploitation.
- **Analyseur heuristique.** Lors de l'analyse d'un programme quelconque, l'analyseur émule son exécution et enregistre dans un rapport toutes les actions suspectes telles que l'ouverture ou l'enregistrement d'un fichier, l'interception de vecteurs d'interruptions, etc. Sur la base de ce rapport, l'application décide de l'éventuelle infection du programme par un virus. L'émulation a lieu dans un milieu artificiel isolé, ce qui permet d'éviter l'infection de l'ordinateur.
- **Restaurer le système** après les actions malveillantes des logiciels espions grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espions. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!
- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.
- **Protection du système de fichiers** : n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système après une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles

est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques automatiques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer. Le module **Protection des données confidentielles** vous protège contre l'accès non-autorisé aux données personnelles et contre le transfert de celles-ci. Le composant **Contrôle parental** garantit le contrôle de l'accès de l'utilisateur aux sites Internet.

Kaspersky Internet Security 7.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé, toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky® Anti-Virus Mobile

Kaspersky Anti-Virus Mobile garantit la protection antivirus des appareils nomades tournant sous Symbian OS et Microsoft Windows Mobile. Le logiciel est capable de réaliser des analyses antivirus sophistiquées dont:

- **L'analyse à la demande** de la mémoire de l'appareil nomade, de la carte mémoire, d'un répertoire particulier ou d'un fichier distinct. En cas de découverte d'un objet infecté, celui-ci est placé dans le répertoire de quarantaine ou il sera supprimé ;
- **L'analyse en temps réel** : tous les objets entrants ou modifiés sont automatiquement analysés, de même que les fichiers auxquels des requêtes sont adressées ;
- **L'analyse programmée** des informations conservées dans la mémoire de l'appareil nomade ;

- **Protection contre les sms et mms indésirables .**

Kaspersky Anti-Virus for File servers

Ce logiciel offre une protection fiable pour les systèmes de fichiers des serveurs tournant sous Microsoft Windows, Novell NetWare, Linux et Samba contre tous les types de programmes malveillants. Le logiciel contient les applications suivantes de Kaspersky Lab :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-virus for Samba Server.

Avantages et fonctions :

- *Protection des systèmes de fichiers des serveurs en temps réel* : tous les fichiers du serveur sont analysés à chaque tentative d'ouverture ou d'enregistrement sur le serveur.
- *Prévention des épidémies de virus* ;
- *Analyse à la demande* de tout le système de fichiers ou de répertoires ou de fichiers distincts ;
- *Application de technologies d'optimisation* lors de l'analyse des objets du système de fichiers du serveur ;
- *Restauration du système après une infection* ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Respect de l'équilibre de la charge du système* ;
- *Constitution d'une liste de processus de confiance* dont l'activité sur le serveur n'est pas contrôlée par le logiciel ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Enregistrement des copies de sauvegarde des objets infectés ou supprimés* au cas où il faudra les restaurer ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Notifications des événements* survenus dans l'utilisation du logiciel par l'administrateur du système ;

- *Génération de rapports détaillés ;*
- *Mise à jour automatique des bases de l'application.*

Kaspersky Open Space Security

Kaspersky Open Space Security est un logiciel qui adopte une nouvelle conception de la sécurité des réseaux des entreprises de n'importe quelle taille dans le but d'offrir une protection centralisée des systèmes d'informations tout en prenant en charge les utilisateurs nomades et les télétravailleurs.

Cette application est composée de quatre logiciels :

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Voici une description détaillée de chacun d'entre eux.

Kaspersky WorkSpace Security est un logiciel conçu pour la protection centralisée des postes de travail dans le réseau d'entreprise et en dehors de celui-ci contre tous les types de menaces modernes présentes sur Internet : Virus, logiciels espions, pirates informatiques et courrier indésirable.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable. ;*
- *Défense proactive* contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Pare-feu personnel* avec système d'identification des intrusions et de prévention des attaques de réseau ;
- *Annulation des modifications malveillantes dans le système ;*
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable ;*
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Analyse du courrier électronique et du trafic Internet* en temps réel ;

- *Blocage des fenêtres pop up et des bannières publicitaires pendant la navigation sur Internet ;*
- *Travail en toute sécurité dans les réseaux de n'importe quel type, y compris les réseaux Wi-Fi ;*
- *Outils de création d'un disque de démarrage capable de restaurer le système après une attaque de virus ;*
- *Système développé de rapports sur l'état de la protection ;*
- *Mise à jour automatique des bases ;*
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits ;*
- *Optimisation du fonctionnement de l'application sur les ordinateurs portables (technologie Intel® Centrino® Duo pour ordinateurs portables) ;*
- *Possibilité de réparation à distance (technologie Intel® Active Management, composant Intel® vPro™).*

Kaspersky Business Space Security offre une protection optimale des ressources informatiques de l'entreprise contre les menaces Internet modernes. Kaspersky Business Space Security protège les postes de travail et les serveurs de fichiers contre tous les types de virus, de chevaux de Troie et de vers, prévient les épidémies de virus et garantit l'intégrité des informations ainsi que l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Administration à distance de l'application, y compris l'installation, la configuration et l'administration ;*
- *Compatibilité avec Cisco® NAC (Network Admission Control) ;*
- *Protection des postes de travail et des serveurs de fichiers contre tous les types de menaces Internet ;*
- *Utilisation de la technologie iSwift pour éviter les analyses répétées dans le cadre du réseau ;*
- *Répartition de la charge entre les processeurs du serveur ;*
- *Isolement des objets suspects du poste de travail dans un répertoire spécial ;*
- *Annulation des modifications malveillantes dans le système ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Défense proactive des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;*

- *Analyse du courrier électronique et du trafic Internet en temps réel ;*
- *Pare-feu personnel avec système d'identification des intrusions et de prévention des attaques de réseau ;*
- *Protection lors de l'utilisation des réseaux sans fil Wi-Fi ;*
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants ;*
- *Isolement des objets suspects dans un répertoire spécial ;*
- *Mise à jour automatique des bases.*

Kaspersky Enterprise Space Security

Ce logiciel propose des composants pour la protection des postes de travail et des serveurs contre tous les types de menaces Internet modernes, supprime les virus du flux de messagerie, assure l'intégrité des informations et l'accès instantané de l'utilisateur aux ressources du système.

Avantages et fonctions :

- *Protection des postes de travail et des serveurs contre les virus, les chevaux de Troie et les vers ;*
- *Protection des serveurs de messagerie Sendmail, Qmail, Postfix et Exim ;*
- *Analyse de tous les messages sur le serveur Microsoft Exchange y compris les dossiers partagés ;*
- *Traitement des messages, des bases de données et d'autres objets des serveurs Lotus Domino ;*
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable ;*
- *Prévention des épidémies de virus et des diffusions massives ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Administration à distance de l'application, y compris l'installation, la configuration et l'administration ;*
- *Compatibilité avec Cisco® NAC (Network Admission Control) ;*
- *Défense proactive des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;*
- *Pare-feu personnel avec système d'identification des intrusions et de prévention des attaques de réseau ;*
- *Utilisation sécurisée des réseaux sans fil Wi-Fi ;*

- *Analyse du trafic Internet* en temps réel ;
- *Annulation des modifications malveillantes* dans le système ;
- *Redistribution dynamique des ressources* lors de l'analyse complète du système ;
- *Isolement des objets suspects* dans un répertoire spécial ;
- *Système de rapports* sur l'état de la protection ;
- *Mise à jour automatique des bases*.

Kaspersky Total Space Security

Le logiciel contrôle tous les flux de données entrant et sortant : courrier électronique, trafic Internet et interaction dans le réseau. Le logiciel prévoit des composants pour la protection des postes de travail et des périphériques nomades, garantit l'accès instantané et sécurisé des utilisateurs aux ressources informatiques de l'entreprise et à Internet et garantit également une communication sûre via courrier électronique.

Avantages et fonctions :

- *Protection intégrale contre les virus, les logiciels espions, les pirates informatiques et le courrier indésirable* à tous les niveaux du réseau de l'entreprise : depuis les postes de travail jusqu'aux passerelles d'accès Internet ;
- *Défense proactive* des postes de travail contre les nouveaux programmes malveillants dont les définitions n'ont pas encore été ajoutées aux bases ;
- *Protection des serveurs de messagerie et des serveurs de coopération* ;
- *Analyse du trafic Internet* (HTTP/FTP) qui arrive sur le réseau local en temps réel ;
- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Blocage de l'accès depuis un poste de travail infecté* ;
- *Prévention des épidémies de virus* ;
- *Rapports centralisés* sur l'état de la protection ;
- *Administration à distance* de l'application, y compris l'installation, la configuration et l'administration ;
- *Compatibilité avec Cisco® NAC* (Network Admission Control) ;
- *Compatibilité avec les serveurs proxy matériels* ;
- *Filtrage du trafic Internet* selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;

- *Utilisation de la technologie iSwift pour éviter les analyses répétées dans le cadre du réseau ;*
- *Redistribution dynamique des ressources lors de l'analyse complète du système ;*
- *Pare-feu personnel avec système d'identification des intrusions et de prévention des attaques de réseau ;*
- *Travail en toute sécurité dans les réseaux de n'importe quel type, y compris les réseaux Wi-Fi ;*
- *Protection contre les tentatives d'hameçonnage et le courrier indésirable ;*
- *Possibilité de réparation à distance (technologie Intel® Active Management, composant Intel® vPro™) ;*
- *Annulation des modifications malveillantes dans le système ;*
- *Technologie d'autodéfense de l'antivirus contre les programmes malveillants ;*
- *Compatibilité absolue avec les systèmes d'exploitation 64 bits ;*
- *Mise à jour automatique des bases.*

Kaspersky Security for Mail Servers

Ce logiciel a été développé pour la protection des serveurs de messagerie et des serveurs de coopération contre les programmes malveillants et le courrier indésirable. Le logiciel contient des applications pour la protection de tous les serveurs de messagerie populaires : Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix et Exim et il permet également d'organiser la répartition des passerelles de messagerie. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel ;*
- *Filtrage des messages non sollicités ;*
- *Analyse des messages et des pièces jointes du courrier entrant et sortant ;*

- *Analyse antivirus de tous les messages sur le serveur Microsoft Exchange y compris les dossiers partagés ;*
- *Analyse des messages, des bases de données et d'autres objets des serveurs Lotus Domino ;*
- *Filtrage des messages en fonction du type de pièce jointe ;*
- *Isolement des objets suspects dans un répertoire spécial ;*
- *Système convivial d'administration du logiciel ;*
- *Prévention des épidémies de virus ;*
- *Surveillance de l'état du système de protection à l'aide de notifications ;*
- *Système de rapports sur l'activité de l'application ;*
- *Montée en capacité de l'application dans le cadre des ressources disponibles dans le système ;*
- *Mise à jour automatique des bases.*

Kaspersky Security for Internet Gateway

Ce logiciel garantit un accès sécurisé au réseau Internet pour tous les membres de l'organisation. Il supprime automatiquement les programmes malveillants et les programmes présentant un risque potentiel de tous les flux de données qui arrivent dans le réseau via le protocole HTTP/FTP. La solution contient :

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Voici quelques-unes de ses fonctions :

- *Protection fiable contre les programmes malveillants et présentant un risque potentiel ;*
- *Analyse du trafic Internet (HTTP/FTP) en temps réel ;*
- *Filtrage du trafic Internet selon une liste de serveurs de confiance, le type d'objets et le groupe d'utilisateurs ;*
- *Isolement des objets suspects dans un répertoire spécial ;*
- *Système convivial d'administration ;*
- *Système de rapports sur le fonctionnement de l'application ;*
- *Compatibilité avec les serveurs proxy matériels ;*

- *Montée en capacité de l'application* dans le cadre des ressources disponibles dans le système ;
- *Mise à jour automatique des bases.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper offre une analyse antivirus rapide du trafic sur les serveurs qui utilisent Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Le programme se présente sous la forme d'un module externe et il analyse et traite en temps réel les messages entrants et sortants.

B.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://case.kaspersky.fr/
-------------------	---

Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com
---------------------------	--

ANNEXE C. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN UTILISANT LE CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'UTILISEZ PAS LE CD, NE TELECHARGEZ PAS, N'INSTALLEZ PAS ET N'UTILISEZ PAS CE LOGICIEL.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel qui vous sera fournie par Kaspersky Lab comme faisant partie du Logiciel.

1. *Octroi de la Licence.* Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 *Utilisation.* Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de cet ordinateur. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

2. Assistance technique.

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

3. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Lab et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de

propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

4. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Lab reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

5. *Limites de Garantie.*

- (i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première installation d'un logiciel kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.
- (ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Lab ne garantit pas que le Logiciel et/ou la Documentation répondent à ces besoins et que leur utilisation soit exempte d'interruptions et d'erreurs.
- (iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus connus ou qu'il n'affichera pas de message de détection erroné.
- (iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.
- (v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat.
- (vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce

paragraphe (vi) ont effet entre Kaspersky Lab et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

6. Limites de Responsabilité.

- (i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.
- (ii) Selon les termes du paragraphe (i) au-dessus, Kaspersky Lab ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):
 - (a) Perte de revenus;
 - (b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);
 - (c) Perte de moyens de paiement;
 - (d) Perte d'économies prévues;
 - (e) Perte de marché;
 - (f) Perte d'occasions commerciales;
 - (g) Perte de clientèle;
 - (h) Atteinte à l'image;
 - (i) Perte, endommagement ou corruption des données; ou
 - (j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).
- (iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Lab (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet.

Le support technique, tel que présenté en clause 2 de cet EULA ne vous concerne pas si vous utilisez ce programme en mode de démonstration ou d'essai. De même vous n'avez pas le droit de vendre les éléments de ce programme, ensembles ou séparément.

Vous pouvez utiliser le logiciel pour des raisons de démonstration ou d'essai pour la période spécifiée dans la licence. La période d'essai ou de démonstration commence à l'activation de la licence ou dès son installation. La période est visible dans l'interface graphique windows du logiciel.